ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Security Enhancement using Dynamic Cache on DSR Based MANETS

Saurabh Mittal
Sr. Assistant Professor
Department of Computer Science and Engineering, Haryana College of Technology and Management
Kaithal, India
mittal_saurabhin@yahoo.co.in

Sapna Boora*
M.Tech (CSE)
Department of Computer Science and Engineering, Haryana College of Technology and Management
Kaithal, India
sapnaboora@gmail.com

Abstract: In the DSR Routing Algorithm, when a node needs to transmit a packet to some other node it has to find the route every time. If the route is not found, then the node generates a route request (RREQ) which has (Source id, destination id, sequence number and route number). When a node receives a RREQ , the node searches for available routes to the destination from its route cache. If it finds an available route, a node sends a route reply packet (RREP), which contains route information from the source to the destination, to the source. Otherwise, it appends its id to the source route in the RREQ and rebroadcasts the RREQ. Thus black hole node attacks the network at the time of route finding and start acting as if it has the correct path for the destination. This cause serious problem in the operations and services of the networks .They may lead to the problem of system failure in terms of network availability. It makes the ad hoc node unable to transmit and receive information. This eventually brings down the overall performance of the network. Current solutions may either found the intrusion too late or produce a heavy network overhead .Many solutions are assuming as if there is only one black hole node in the network but black hole attack can be cooperative. A black hole attack and DOS attack increases network overhead, decreases the network's lifetime by boosting energy consumption, and finally destroys the network. We are representing the solution for above problem

Keywords: Adhoc Network, DSR (Dynamic Source Routing), Caching, DOS (Denial of Service), Blackhole, Security

I. INTRODUCTION

A. Wireless Networks:

Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. Wireless networks can be classified in two types: Infrastructure network and Infrastructure less (ad hoc) networks. These are defined as follows:

a. Infrastructure Networks: In the infrastructure-based network communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes. The access point does not just control medium access, but also acts as a bridge to other to wireless or wired networks. The base stations are fixed as the node goes out of the range of a base station; it gets into the range of another base station. The cellular networks are infrastructure-based network.

b. Infrastructure Less Networks: Ad-hoc wireless network do not need any infrastructure to work .Each node can communicate directly with other node so no access point controlling medium access is necessary. Infrastructure less networks, do not have fixed routers all the nodes in the network need to act as routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Mobile Ad hoc Networks (MANET) are example of infrastructure less network.

B. Manet's (Mobile Adhoc Networks):

With the advancement in radio technologies like Bluetooth, IEEE 802.11 or HIPERLAN, a new concept of networking has emerged. This is known as ad hoc networking where potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication. Nodes within ad hoc are mobile and they communicate with each other within radio range through direct wireless links or multihop routing. A

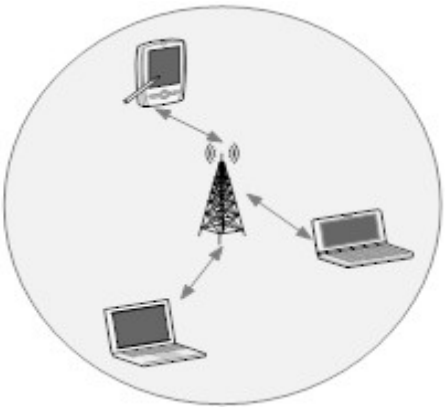

Figure 1. Centralized topology network

Mobile Ad hoc network or MANET is defined as a wireless network of mobile nodes communicating with each other in a multi-hop fashion without the support of any fixed infrastructure such as base stations, gateways or access points.

For this reason, MANETs are also called infrastructure less or non-infrastructure wireless networks. The term ad hoc implies that this network is a network established for a special, often extemporaneous service customized to specific applications. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure; or, if there is an infrastructure, it is not adequate or cost effective. The absence of a central coordinator and base stations makes operations in MANETs more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks (WiFi networks). In MANETs, routing and

resource management are done in a distributed manner; that is, all nodes coordinate to enable communications among themselves. This requires each node to be more intelligent so that it can operate both as a network host for transmitting and receiving data, and as a network router for forwarding packets for other nodes.

There are currently two type of mobile wireless networks. The first is known as the infrastructure Centralize Topology or as a fixed structure networks as shown in Figure 1. The bridges for these networks are known as base stations (BS). A mobile node within these networks connects and communicates with the nearest BS that is within transmission range. As the mobile goes out of range of one BS and enters into the range of another, a "hand off" occurs from the old BS to the new BS, and the mobile is able to continue communication seamlessly throughout the network. The second type of mobile wireless network is the infrastructure less or (Uncentralize Topology) networks have no fixed structure, commonly known as Mobile ad hoc network (MANETs) or Ad hoc networks.

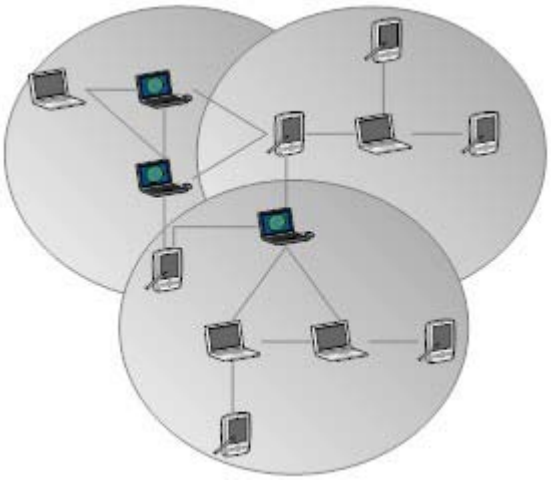

Figure 2. Uncentralized topology network

A MANET, due to its unique infrastructure less characteristic feature, compared to other types of wireless networks, can be very useful for many applications in which no infrastructure exists. Establishing communication among a group of soldiers in a battlefield is a good example. A fixed infrastructure in enemy territories or in hostile terrains may not be possible. In such environments, MANETs can provide the required communication. In addition, applications in this area requires a secure communication as eavesdropping or other security threats can compromise the network and threaten the safety of personnel involved in these military operations. Secure multicast may also be required. For example, the leader of a group of soldiers may want to give an order to all the soldiers, or to a set of selected personnel. Hence, routing protocols in such applications are required to provide secure communication with support for multicast routing. Another area in which MANETs can be deployed is collaborative and distributed computing.

II. ADHOC ROUTING PROTOCOL

A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.The world of ad hoc protocols is evolving very fast and new drafts pop-up all the time. Routing is mainly classified into static routing and dynamic routing. Static routing refers to the routing strategy being stated manually or statically, in the router. Static routing maintains a routing table usually written by a networks administrator. The routing table doesn't depend on the state of the network status, i.e., whether the destination is active or not. Dynamic routing refers to the routing strategy that is being learnt by an interior or exterior routing protocol. This routing mainly depends on the state of the network i.e., the routing table is affected by the activeness of the destination. The major disadvantage with static routing is that if a new router is added or removed in the network then it is the responsibility of the administrator to make the necessary changes in the routing tables. But this is not the case with dynamic routing as each router announces its presence by flooding the information packet in the network so that every router within the network learn about the newly added or removed router and its entries. Similarly this is the same with the network segments in the dynamic routing.

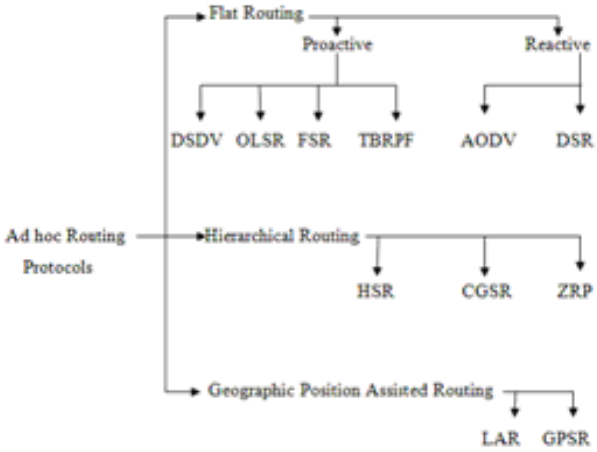

Figure 3. Classification of Routing Protocols in Manets

A. Dynamic Source Routing (DSR):

DSR adopts a similar on-demand approach as AODV regarding the route discovery and maintenance processes. A key difference of DSR from AODV and other ondemand protocols is the use of source routing, where the source node specifies the complete sequence of intermediate nodes for each data packet to reach its destination. The source-route information is carried by the header of the data packet. The advantage of source routing is that no additional mechanism is needed to detect routing loops. The obvious disadvantage is that data packets must carry source routes. The data structure DSR uses to store routing information is route cache, with each cache entry storing one specific route from the source to a destination.

a. DSR Route Discovery: In route discovery source node is wishing to send a packet to a destination node obtains a source route to destination**.** Route Discovery is used only when source node attempts to send a packet to destination node and does not already know a route to

destination when any host receives a route request packet (RREQ). It processes the request according to the following steps.

i. The source broadcasts a ROUTE REQUEST.
ii. If the node has a route to the source, it sends a ROUTE REPLY to the source, Including the source route in the ROUTE REQUEST and the cached route
iii. If the node has no such a route, it adds its address to the source route in the packet header and rebroadcasts the ROUTE REQUEST.
iv. The destination receives the ROUTE REQUEST, and sends a ROUTE REPLY containing the route to the source.
v. Each node forwarding the ROUTE REPLY caches the route starting from itself to the destination.
vi. The source receives the ROUTE REPLY, and caches the source route.

b. DSR Route Maintenance: In route maintenance source node is able to detect, while using a source route to destination**,** if the network topology has changed such that it can no longer use its route to destination because a link along the route no longer works. When Route Maintenance indicates a source route is broken, source can attempt to use any other route it happens to know to destination, or can invoke Route Discovery again to find a new route.

i. A node forwarding a packet is responsible for confirming that the packet has reached the next hop in the route.
ii. If no acknowledgement is received after the maximum number of retransmission attempts, this node assumes that the next hop is unreachable and sends a ROUTE ERROR to the source node, indicating the broken link.
iii. Each node receiving a ROUTE ERROR removes from its cache the routes containing the broken link.

III. WORKING CONCEPTS

A. Integation of Information:

[1], provide a brief overview of the concept of DSR (Dynamic Source Routing Protocol) The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. [2], proposed the cooperating caching technique, this article represents the cooperative caching techniques which allows the sharing and coordination of cached data among multiple nodes and also supports data access in ad hoc networks.

We proposed three schemes: Cache Path, Cache Data, and Hybrid Cache. In Cache Data, intermediate nodes cache the data to serve future requests. In Cache Path, mobile nodes cache the data path and use it to redirect the future requests to the nearby nodes instead of the data center. Hybrid Cache takes advantage of both while avoiding their weaknesses. [3], proposed the active packets improvement. DSR is an on-demand method that floods route requests when the route is needed. Route caches in DSR are used to reduce flooding of route requests. But with increase in network size and node mobility, cached routes become stale and inefficient. This paper represents a deployable active network approach to this route cache problem. In this method, an active packet roams around the netwok, and collects network topology information. With this we not only adjust the existing routes, but also cache future routes based on the topology information. Thus both route request flooding for the stale routes and the new routes are reduced and also reduces the routing overhead. [4], proposed the NGDC technique. This paper proposed a neighbour group data caching scheme called Neighbour Group Data Caching (NGDC) for improving data access efficiency in MANETs. The objective is to improve data availability and access efficiency by collaborating local resources of mobile nodes.

To improve this, cooperative caching discovers data sources which induce less communication cost by utilizing neighbour group nodes. Mobile hosts maintain the localized caching status among the group members and store different data objects. [5], provide the concept of intelligent caching. This paper presents an analysis of the effect of caching in a non clustered network using on-demand routing protocols. This technique helps in storing more number of routes that are learnt without erasing the entries in the cache, to store a new route that is learnt. Intelligent caching is a technique in which a node not only saves the path discovered during route discovery for itself but also for others who are located close to it. This technique reduces the number of route request packets unnecessarily circulating in the network and also increases the available memory for caching the routes discovered without affecting the performance of DSR. [6] provide the concept of security using SRP. This paper proposes the enhancements in DSR to provide secured route discovery and improved QoS.

The paper evaluates integration of Secured Routing Protocol (SRP) and Secured Message Transmission (SMT) with DSR to get Secured Dynamic Source Routing (S-DSR), which is capable of secured route discovery. The proposed extension also incorporates concurrent usage of multiple cached routes for improved throughput and explores possible enrichment to route cache management resulting in improved efficiency.

[7], DSR is a widely used routing protocol for mobile ad hoc networks, but has very low delivery rates and poor performance in lightly loaded networks with high node mobility. Several of the modifications proposed in the literature such as turning off intermediate node replies improves the performance somewhat. This paper presented three simple (and used in other routing protocols) techniques—limiting replies sent by destination, keeping only one route per destination, and preferring fresher routes over shorter ones—to further improve the performance of DSR. Factorial analysis indicates that both limited replies and one route per destination improve performance significantly and the third feature does not impact performance. While multiple routes may benefit at higher traffic loads, keeping only one route per destination helps sender nodes gather routes when the topology changes.

Additional factorial analysis indicates that, besides routing protocol features, network density impacts the overall performance measurably. [8], proposed the performance of caching strategies. Using an on-demand protocol called “Dynamic Source Routing” (DSR) study the

problem of keeping the caches up-to-date. Previous studies have shown that cache staleness in DSR can significantly degrade the performance. In their work they evaluated three techniques to improve cache correctness in DSR namely wider error notification, route expiry mechanism with adaptive timeout selection and the use of negative caches. The future work will concentrate on modifying the cache model in DSR so that the relative freshness of cached routes can be determined. [9], proposed the link failure algorithm.

Most number of data packets loss is experienced in the Adhoc networks due to Transfer control protocol(TCP)'s high channel error rate and link failure. To improve TCP performance in Adhoc networks a number of schemes have been proposed, where Adhoc networks use the multi-hop wireless connectivity, where the network has quickly changing network topology. ELFN (Explicit Link Failure Notification) is one mechanism to manage link failures with dynamic cache update scheme to improve the TCP performance considerably. In this paper, we propose a mechanism which significantly increases the throughput of TCP's performance with ELFN based Dynamic cache update scheme using Dynamic source routing protocol. In this paper, they proposed an ELFN-based Dynamic cache update mechanism. It provides dynamic probing of probe packet and helps in quickly continuing the use of channel in link failure cases which are not due to route failure but due to channel contention.

They implemented proposed Dynamic cache update mechanism in ns-2 network simulator. [10], DoS attacks are hard to detect and easy to implement by an attacker. These are considered to be the most vulnerable category of attacks for network layer, hence requires more attention. Entire network may fail in presence of such an attack. In black hole attack, an attacker first introduce itself in the forwarding group (e.g., by implementing rushing attack), or by any other means and then instead of forwarding the data packet to the proper destination, it simply drops all the packets it receive resulting a poor packet delivery ratio. Grey Hole is a node that can switch from behaving correctly to behaving like a black hole. This is done to avoid detection. In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network. [11],

The black hole problem is one of the security attacks that occur in mobile ad hoc networks (MANETs).They represented two possible solutions. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. In this solution, the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route is identified. Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not.

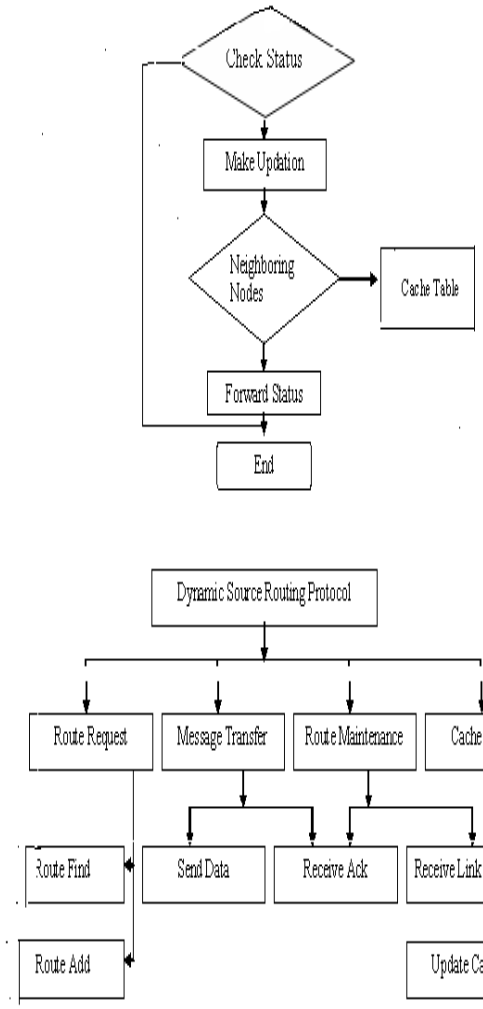

Figure 4. Cache Updation

[12], Denial of service (DoS) attack is a major class of security threats today. They consume resources of remote hosts or network and make them deny or degrade services for legitimate users.. Therefore, nodes in MANETs are more vulnerable to DoS attacks. In this paper, they proposed a zone sampling-based traceback (ZSBT) algorithm for tracing DoS attackers in MANETs. In this algorithm, when a node forwards a packet, the node writes its zone ID into the packet with a probability. After receiving these packets, the victim can reconstruct the path between the attacker and itself. After the attacker has been traced, the victim can take several measures to prevent the attack First, the victim can inform the zone path to which the nodes belong not to forward or reduce the priority of packets from the zone where the attacker stays. Second, if the position-based routing protocol is used in the network, the victim can send a routing error message to the nodes in the attacker's zone.

Thus, the attacker will stop sending packets to the victim because it thinks that the victim is unreachable. Lastly, if there is an out-of-band communication method, the victim can inform the nodes in the attacker' zone that one of you has been compromised. [13], An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructureless. A black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. The damage will be serious if malicious nodes work together as a group. This type of

attack is called cooperative black hole attack. The performance has been analyzed by varying the number of mobile nodes and black hole nodes. Therefore the work can be extended by implementing some mechanisms to detect the Black Hole attack. Improvement for overcoming the effect of Black Hole should orient towards controlling the delay.

IV. METHODOLOGY

In this research work we will represent the simulation of DSR protocol with caching on NS2 Simulator. We are modifying the link failure algorithm by performing the delay analysis thereby reducing the intrusion attack and avoids the congestion on node.

A. Observe the actual throughput in congestion and without congestion.
B. Observe the ouput with expected ouput.
C. If there is some weaker node that performed delayed data transmission, we need to identify that node.
D. Eliminate the delayed node.
E. Adapts quickly to routing change by immediate updation of cache table of all nearby nodes.
F. Reduce congestion over the network.
G. No requirement for bidirectional transmissions.

V. CONCLUSION

We implemented our work on simulation model.Various researchers use different simulation models such as Opnet, GloMoSim, NS-2 etc, and we are using the ns-2 for evaluating the proposed routing protocol.In this work This work introduces an approach based on immune networks to analyze the network traffic, which focuses on the broken link problem in a network. The idea behind the proposed approach is to dynamically cluster the network traffic and monitor activity of the clusters to look for dominating features of the traffic . Such approach allows in the first place to gather information about incoming, or proceeding attack, to take the most efficient countermeasures against the threat. The broken link problem can occur because of different reasons such as some intrusion attack like DOS, black hole etc. It can be because of low energy of the node etc. In this proposed system we will first analyse the network detect if there is some misbehaving node based on the current statistics of receiving packets, forwarding packets and droping packets.

Once the drop rate crosses the threshold value it is taken as the droping node and the DSR cache will be updated as assuming it misbehaving node. Now the data will be transferred from some compromising node. This way we are getting the secured data transmission oner the entire network.

VI. REFERENCES

[1] D. B. Johnson D. A. Maltz Josh Broch, "The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad-hoc Networks," Journal on Mobile Computing, pp 153-186, 1996

[2] Liangzhong Yin and Guohong Cao," Supporting Cooperative Caching in Ad Hoc Networks**,"** IEEE INFOCOM, 2004, pp 7803-8356**.**

[3] Y. H. Steven Berson, "Active Packets Improve Dynamic Source Routing for AD Hoc Networks," Deptt of Computer Science University of Southern California, Information Sciences Institute University of Southern California.

[4] Mrs. K. Shanmugavadivu and Dr. M. Madheswaran,"Caching Technique for Improving Data Retrieval Performance in Mobile Adhoc Networks,"

[5] Shobha K.R., and K. Rajanikanth, **"**Intelligent Caching in on-demand Routing Protocol for Mobile Ad Hoc Networks**,"** World Academy of Science, Engineering and Technology, pp.413-420, 2009

[6] Rajendra V. Boppana Anket Mathur, "Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks**"** Workshop on Next Generation Wireless Networks, pp 1-8, December 2005

[7] A. Rawat, P. Dattatraya Vyavahare, and A. K. Ramani, " Enhanced DSR for MANET with Improved Secured Route Discovery and QoS**,**" International Journal of Network Security, Vol.5, No.2, PP.158–166, Sept. 2007.

[8] K. Marina,"Performance of Route Caching Strategies in DynamicSource Routing**,**"Deptt of Electrical & Computer Science & Engg, University of Cincinnati, 2003

[9] S.C. Shinde, J. Vinayak,"An Explicit Link Failure Notification With Dynamic Cache Update Scheme To Improve Tcpperformance Using Dsr Protocol In Manets", International Journal of Engineering Science and Technology Vol. 2(6), 2010, pp.2263-2271

[10] Niki Devi, ATTACKS ON WIRELESS MANET, International Journal of Information Technology and Knowledge Management, 2008 pp. 569-571.

[11] M Al-Shurman, S Moo Yoo, Black Hole Attack in Mobile Ad Hoc Networks, april 2004,pp 96-99

[12] X.J Yaoxue Zhang, ZSBT: A Novel Algorithm for Tracing DoS Attackers inMANETs, EURASIP Journal onWireless Communications and Networking, 2006,pp 1-9

[13] A Saini, H. Kumar, Effect Of Black Hole Attack In Manets**,** IJCST Vol. 1, Iss ue 2, December 2010

[14] The Institute of Electrical and Electronics Engineers, Inc. IEEE Std 802.11 – "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," 1999 edition.