Volume: 03, Issue: 01, Pages:1035-1043 (2011)

Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme

Rusha Nandy
Department of Information Technoloy, Calcutta Institute of engineering and Management, Kolkata-40
Email: rinku2008.rusha @gmail.com
Debdutta Barman Roy
Department of Information Technoloy, Calcutta Institute of engineering and Management, Kolkata-40
Email: barmanroy.debdutta@gmail.com

----------ABSTRACT----------
An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are capable of communicating with each other without the use of a network infrastructure or any centralized administration. Due to open medium, dynamic topology, distributed cooperation, constrained capabilities ad hoc networks are vulnerable to many types of security attacks; one such attack is rushing attack. It is a malicious attack that is directed against on demand routing protocols that uses duplicate suppression at each node.

Keyword**: Attacks, DSR protocol, Manet, Rushing Attack, Self organization based Clustering scheme.**

Date of Submission: March 13, 2011 Date of Acceptance: May 13, 2011

1. INTRODUCTION

A mobile ad-hoc network or MANET is an autonomous system of mobile routers (and associated hosts) connected by wireless links-the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily. Thus, the network's wireless topology may change rapidly and unproductively .Such a network is developed in 'Ad-hoc' basis without any pre-existing infrastructure and may operate in either stand alone fashion or may be connected to the larger Internet.

1.1Characteristics of MANETs

- Communication is via wireless means(generally via radio waves)
- Nodes can perform the roles of both hosts and routers
- No centralized controller and infrastructure. Intrinsic mutual trust
- Dynamic network topology. Frequent routing updates
- Autonomous, no infrastructure needed.
- Can be set up anywhere
- Energy constraints are of important consideration
- Security is limited.

1.2 Application areas

- Military or police exercises
- Disaster relief operations
- Mine site operations
- Urgent business meetings
- Robot data acquisition

1.3 Security Issues in Manet

MANETs are much more vulnerable to attack than wired networks. This is because of the following reasons [7].

- Open Medium: Eavesdropping is much easier than in wired network

- Dynamically changing network topology: Mobile node comes and goes from the network, thereby allowing any malicious node to join the network without being detected.

1.4 Merits of MANET

- They provide access to information and services regardless of geographic position.

- These networks can be set up at any place and time.

- These networks work without any pre-existing infrastructure.

Volume: 03, Issue: 01, Pages:1035-1043 (2011)

1.5 Demerits of MANET

- Limited resources: Limited resource invokes the problem of limited security
- Lack of authorization facilities: Intrinsic mutual trust is vulnerable to attacks
- Time varying topology: Volatile, changing network topology makes it hard to detect malicious nodes.
- Security protocols for wired network can not work for ad-hoc networks.

2. ATTACKS IN MANETS

Attacks in MANETs can be classified as:

- Passive attack
- Active attack

2.1 Passive attack

A passive attack does not actually disrupt the operation of the operation of the network.

E.g. Snooping: Snooping is unauthorized access to another person's data.

2.2 Active attack

An active attack attempts to alter or destroy the data being exchanged in the network [1], [8].

2.3 Layer based attack

Network Layer Attack: The list of different types of attacks on network layer is discussed hereby:

• Wormhole Attack: In wormhole attack, a malicious node, receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as wormhole.

• Black hole Attack: An attacker listen the requests for the routers in a flooding based protocol .When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route and enters into the pathway to do anything with the packets passing between them.

• Byzantine Attack: In this attack, a compromised intermediate node or a asset of compromised intermediate nodes works in collision and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which result in disruption or degradation of the routing services.

• Resource Consumption Attack: In this attack, an attacker tries to consume or waste away resources of the other nodes present in the network. The resources that are targeted are:

- Battery power
- Band width
- Computational power

- Routing Attack: There are several attacks which can be mounted on the routing protocols and may disrupt the proper operation of the network [2].

Brief description of such attacks is given below:

i. Routing Table Overflow: In this case, the attacker create routes to nonexistent nodes, the goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation.

ii. Packet replication: In this case, an attacker replicates stale packets.

iii. Route Cache Poisoning: In the case the route cache is destroyed or damaged

iv. Rushing Attack: On-Demand Protocols (such as AODV or DSR) that use duplicate suppression during the route discovery process are vulnerable to this attack.

Transport Layer Attack:

- Session Hijacking: At first the attacker spoofs the IP address of target machine and determines the correct sequence number. After that he performs s DOS attack on the victim. As a result the target system becomes unavailable for sometime. The attacker now continues the session with the other system as a legitimate system [11].

Application Layer Attack:

- Repudiation: In simple term, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication.

2.4 Multi Layer Attack:

•Denial of service (DoS): In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network.

•Jamming: In this form of attack, the attacker initially keeps monitoring the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. It then transmits signals on that frequency so that error free reception at the receiver is hindered.

•SYN Flooding: In this form of attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return address of the SYN packets.

•Distributed DOS Attack: Distributed Denial of Services is more severe form of DoS.

3. DESCRIPTION OF RUSHING ATTACK

Definition: A rushing attacker exploits the duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group [3].

3.1 Rushing Attack Formation

Algorithm:

Step1: Set of N numbers of node is created.

Step2: Create a connection between nodes.

Step3: Rushing node invaded into the forward multicast Group.

Step4: Send the packet to the particular groups

Step5: At mean time attacker node tap all the packets.

Step6: The packets in the attacker node are then quickly forwarded to the next upcoming node.

Step7: The data packets from the legitimate node reach the destination late and so it is dropped as Duplicate packet.

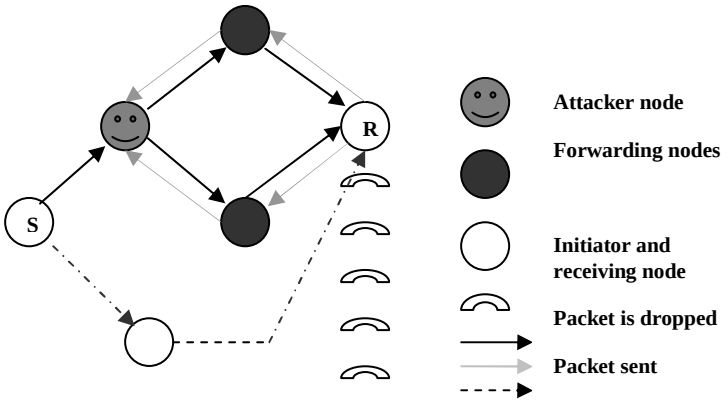

Fig 1: Rushing attack Formation

3.2 Rushing Attack Based On Three Scenarios

3.2.1 Rushing Node At Near Sender

In this figure node S sends the packet to the destination node R. The attacker node A is placed at near sender.

The data packets from the sender are forwarded to both the node A and C at the same time. The attacker nodes quickly forward the data packet to node E than the node C. The attacker node forwards the packet to node E then to G and B node. Finally Receiver R receives the data packets that are forwarded by attacker node. The performance of Attack Success Rate with respect to this scenario is calculated.

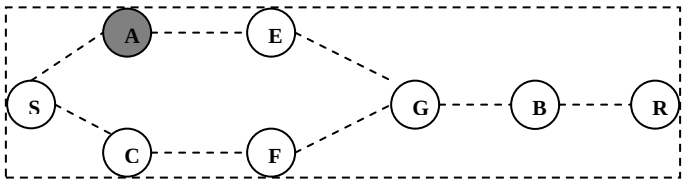

Fig 2: Rushing attacker at near sender

3.2.2 Rushing Node At Near Receiver

this figure node S sends the packet to the destination node R. The attacker node A is placed at near receiver. The sender node forwards the data packets to both the node B and C at the same time. The data packet can pass through either B, E and G nodes or C, F and G nodes. When the data packet reaches the attacker node A, it quickly forwards the data packet to node R. The performance of Attack Success Rate with respect to this scenario is calculated

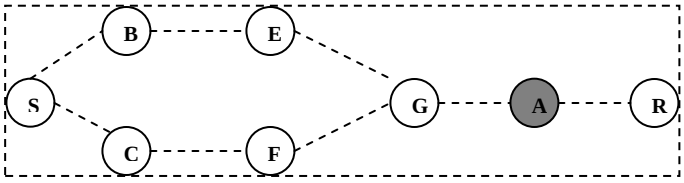

Fig 3: Rushing attacker at near receiver

3.2.3 Rushing Attack at Anywhere within the Network

In this figure node S sends the packet to the destination node R. The attacker node A is placed anywhere within the network. The data packet from the sender is forwarded to the nodes B and C. The data packet is then forwarded through the nodes B and E.

But the data packet passed through the node C and then to attacker node A which quickly forwards the data packet to the node G than from the node E. The data packet is then finally reaches the receiver node R through node F. The performance of Attack Success Rate with respect to this scenario is calculated.

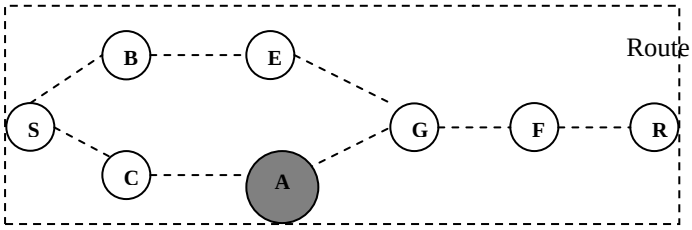

Fig 4: Rushing attacker at anywhere in the network

REASON: ON-DEMAND ROUTING ALGORITHM IS PRONE TOWARDS RUSHING ATTACK

On demand routing protocols delay ROUTE REQUEST forwarding in two ways:

- Medium Access Control (MAC) protocols generally impose delays between when the packet is handed to the network interface for transmission and when the packet is actually transmitted [16].
- Even if the MAC layer does not specify a delay, on-demand protocols generally specify a delay between receiving a REQUEST and forwarding it, in order to avoid collisions of the REQUEST packets.
- Another way that a relatively weak attacker can obtain an advantage in forwarding speed is to keep the network interface transmission queues of nearby nodes full.

4. BRIEF OVERVIEW OF DSR PROTOCOL

Dynamic Source Routing (DSR) is an example of reactive(on-demand) routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence [4],[9].

DSR contains two phases:

•Route Discovery (find a path)

•Route Maintenance (maintain a path)

Route discovery:

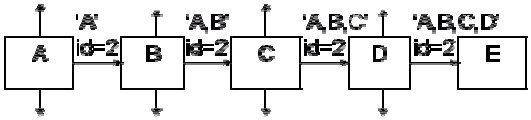

Fig 5: Route discovery process

node A has in his Route Cache a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started:

1. Node A (initiator) sends a RouteRequest packet by flooding the network

2. If node B has recently seen another RouteRequest from the same target or if the address of node B is already listed in the Route Record, Then node B discards the request!

3. If node B is the target of the Route Discovery, it returns a RouteReply to the initiator. The RouteReply contains a list of the "best" path from the initiator to the target. When the initiator receives this RouteReply, it caches this route in its Route Cache for use in sending subsequent packets to this destination.

4. Otherwise node B isn't the target and it forwards the RouteRequest to his neighbors (except to the initiator).

Route Maintenance:

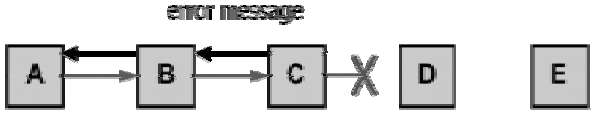

Fig 6: Route Maintenance

Volume: 03, Issue: 01, Pages:1035-1043 (2011)

If node C does not receive an acknowledgement from node D after some number of requests, it returns a RouteError to the initiator A. As soon as node receives the RouteError message, it deletes the broken-link-route from its cache. If A has another route to E, it sends the packet immediately using this new route [12].

Otherwise the initiator A is starting the Route Discovery process again.

5. SELF ORGANIZED CLUSTERING SCHEME

Few important terms:

- Cluster Head: A cluster head, serves as a local coordinator for its cluster, performing Inter-cluster routing, data forwarding and so on.
- Cluster Gateway: A cluster gateway is a non cluster-head node with inter-cluster links, so it can access neighboring Clusters and forward information between clusters.
- Cluster Member: A cluster member is a node that is neither a cluster head nor a cluster gateway.

The proposed self-organized clustering scheme can be divided into cluster formation phase and cluster maintenance phase, which are described in following subsections [6] ,[20].

Pre-requisites and Assumptions:

The prerequisite for our self-organizing scheme includes the use of a proactive routing protocol such as DSDV within the cluster. We define a parameter k that limits the number of hops the node can be away from its cluster head. We assume that the parameter k is known to each node participating in the cluster formation. This hop limit, k, can be tuned based on empirical results and/or dynamically, keeping the mobility into consideration. If the nodes in a MANET are highly mobile, then, the value of k for the cluster can be relatively small as compared to a scenario where mobile nodes in a MANET are stable.

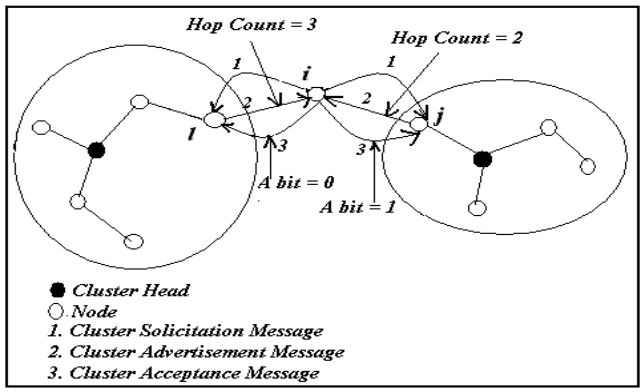

Fig 7: Cluster Formation

Step 1: As shown in Fig when a node i does not belong to any cluster and wants to join a cluster it broadcasts a cluster solicitation message (whose format is shown in Fig 8(a)) to its immediate neighbors.

Step 2: Node j and node l which receive the cluster solicitation message send out a cluster advertisement message whose format is shown in Fig 8 (b). The cluster advertisement of the node j and the node l contains information such as the cluster head ID of the corresponding cluster. It also contains information regarding the number of hops the new node i will be away from the cluster head. Each node maintains its approximate hop count. As shown in Fig 7 the hop count sent by node j to node i in the cluster advertisement is having the value 2 that is its own hop count incremented by one. Similarly the hop count value in the cluster advertisement sent from node l to node i is 3.

Step 3: The node i, after receiving the cluster advertisement(s), first check whether the hop count value in cluster advertisement message is less than k value. Then it chooses the cluster head of the node with the minimum hop count in its advertisement, as its cluster head. Then it sends a cluster acceptance message as shown in Fig 8(c) to the nodes whose cluster advertisements have been received. It sets the A bit to indicate acceptance of advertisement. If the hop count value is the same in two or more cluster advertisements then one of them can be selected randomly.

Step 4: When the new node i receives two or more cluster advertisements from nodes that belong to different clusters, it declares itself as a cluster gateway. It sets the G bit, in the cluster acceptance message. This is shown in Fig 7 with message labeled 3.

Step 5: If the new node i does not receive any cluster advertisement after sending the cluster solicitation message

multiple times or it receives all advertisements with maximum hop count, it declares itself as a cluster head.

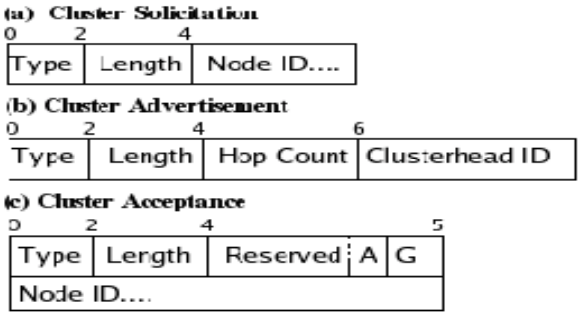

Fig 8: Cluster formation msg format

Cluster Maintenance:

When a new node joins the cluster, it starts advertising itself and after a short time, all nodes in its cluster will have an entry for this node in their routing table. When a node moves out of the range of the cluster, it becomes unreachable to the nodes in the cluster. Thus the entry for this node is deleted from each node's route table within the cluster.

6. SCENARIO OF RUSHING ATTACK IN SELF ORGANISATION BASED CLUSTERING:

Algorithm For Rushing Attacks In Self Organization Based Clustering Scheme:

Step 1: A genuine node tries to enter a cluster of nodes in a Manet

Step 2: The Rushing attacker keeps track from outside.

Step3: Rushing attacker floods the neighboring nodes of the cluster by, not only rushing-ly but also repetitively sending cluster solicitation msg to the aforesaid nodes.

Step4: processing those cluster solicitation msg keeps the neighboring nodes of the cluster busy.

Step 5: The genuine node is deprived of the entry into the cluster.

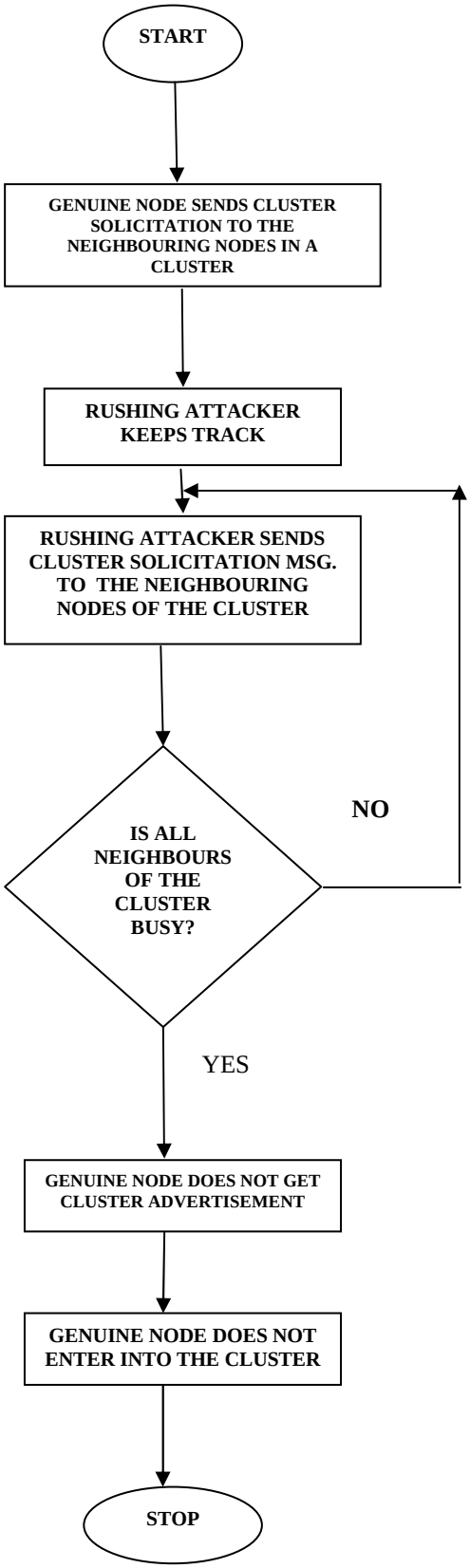

Fig 9 : Flowchart of rushing attack

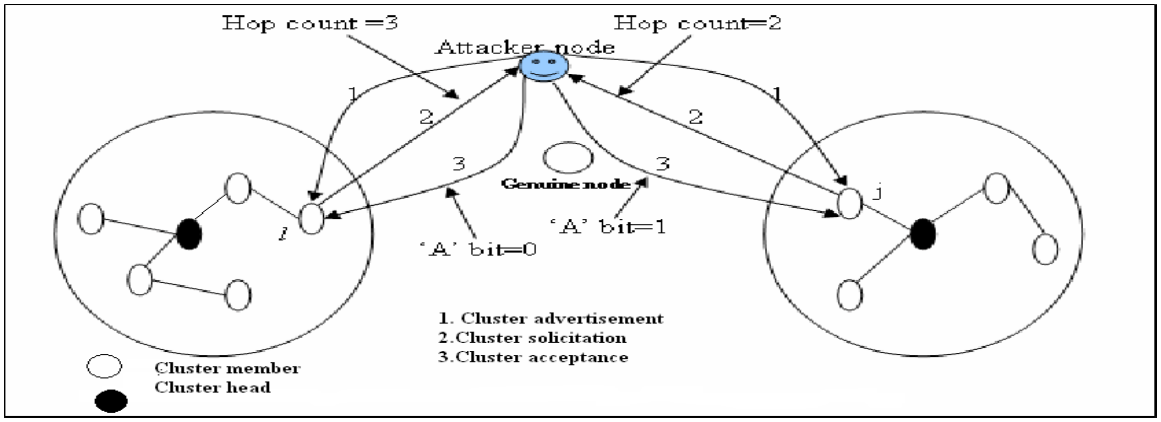

Fig 10: scenario when rushing attacker invades into a self organization based cluster

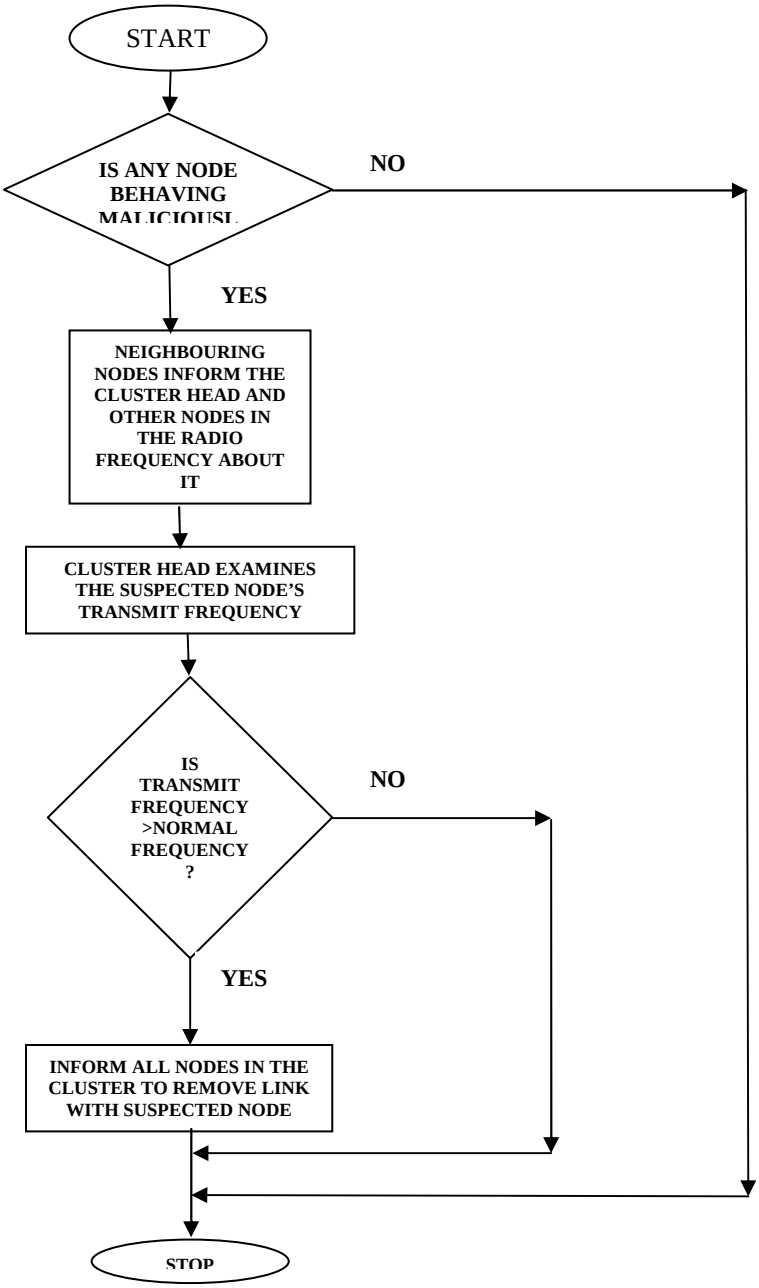

Fig 11: Flowchart for proposed solution to prevent rushing attack

7. PROPOSED SOLUTION FOR RUSHING ATTACK WHEN COMMITTED ON SELF ORGANIZED CLUSTERING SCHEME:

The probable solution includes one calculating metric to determine the transmit frequency of the attacker node. If a node behaves maliciously, the neighboring nodes will report about it to the cluster head. The cluster head will use some metric to determine the transmit frequency of the suspected node .If the transmit frequency of the suspected node is more the normal transmit frequency then the suspected node will be assumed as attacker .the cluster head then informs all nodes present in the cluster to remove link with that attacker node.

Probable Solution of rushing attack when committed on DSR protocol:

One way to thwart an attacker that rushes in this way is to remove delays at both the MAC and routing layers, but this approach does not work against all types of rushing attackers and is not general [5].

For example, in a dense network using a CSMA MAC layer, if a node A initiates a Route Discovery, and B is two hops away from A, and C and D are neighbors of both A and B, then B will likely not receive the ROUTE REQUEST due to a collision between REQUEST forwarded by C and D. In a dense network, such collisions may often prevent the discovery of any nontrivial routes (routes longer than a direct link), which is even more severe than the rushing attack, which prevents the discovery of routes longer than two hops.

8. CONCLUSION AND FUTURE WORKS

As the use of mobile ad hoc networks (MANETs) has increased, the security in MANETs has also become more important accordingly. Historical events show that prevention alone, i.e., cryptography and authentication are not enough; therefore, the intrusion detection systems are brought into consideration. Since most of the current techniques were originally designed for wired networks, many researchers are engaged in improving old techniques or finding and developing new techniques that are suitable for MANETs. With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a co-operative architecture.

In context to the previously discussed solution that has been proposed in this paper the probable future work includes the generation of a metric to calculate the transmit frequency of the nodes in a cluster.

Also, the scenario when the cluster head is suspended from the cluster, the cluster requires a re-election. This situation is yet to be handled.

ACKNOWLEDGEMENT

First and foremost, I would like to thank my guide of this project, Ms. Debdutta Barman Roy for her valuable guidance and advice. Next, I wish to express my sincere thanks to the college (Calcutta Institute of Engineering and Management) authority specifically principal Mr. Swapan Chandra Sarkar and Head of the Department (IT) Mr. Chiranjib Patra for their continuous support and encouragement. Also, I thank the 'West Bengal University of Technology' (WBUT) for offering this subject, for our Project. Finally, an honorable mention goes to my family and friends for their understandings and supports in completing this project.

REFERENCES

[1] Zhang, W. Lee, and Y. Huang, \Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[2] A. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wire- less Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.

[3] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, \Secu- rity in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.

[4] O. Kachirski and R. Guha, \E®ective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, \Mitigating Routing Mis- behavior in Mobile Ad Hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (Mo- biCom'00), pp. 255-265, August 2000.

[6] S. Buchegger and J. Le Boudec, \Performance Analysis of the CONFI-DANT Protocol (Cooperation of Nodes - Fairness in Dynamic Ad-hoc Networks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, June 2002.

[7] Nishu Garg, R.P.Mahapatra. "MANET Security Issues". IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.

[8] Hoang Lan Nguyen, Uyen Trang Nguyen. "A study of different types of attacks on multicast in mobile ad hoc

networks". Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008.

[9] F. Kargl, A. Geiß, S. Schlott, M. Weber. "Secure Dynamic Source Routing". Hawaiian International Conference on System Sciences 38 Hawaii, USA, January 2005.

[10] Jihye Kim, Gene Tsudik. "SRDP: Secure route discovery for dynamic source routing in MANET's".Ad Hoc Networks, Volume 7, Issue 6, Pages 1097-1109, August 2009.

[11] Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

[12] J. Broch et al., "A performance comparison of multi-hop wireless ad hoc network routing protocols" in ACM Mobicom '98, Oct. 1998.

[13] CMU Monarch Group, "CMU Monarch extensions to the NS-2 simulator." Available from http://monarch.cs.cmu.edu/cmuns.html, 1998.

[14] K. Fall and K. Varadhan, "NS notes and documentation." The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC. Available from http://www-mash.cs.berkeley.edu/ns, Nov. 1997.

[15] IEEE Computer Society LAN/MAN Standards Committee, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." IEEE Std. 802.11-1997. IEEE, New York, NY 1997.

[16] S. R. Das, C. E. Perkins, and E. M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," in IEEE Infocom 2000, Mar. 2000.

[17] D. B. Johnson et al., "The dynamic source routing protocol for mobile adhoc networks." IETF Internet Draft. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-02.txt,1999.

[18] Bradley R. Smith and J.J. Garcia-Luna-Aceves. Securing the Border Gateway Routing Protocol. In Global Internet'96, London, UK, November 1996.

[19] Bradley R. Smith, Shree Murthy, and J.J. Garcia-Luna-Aceves. Securing Distance Vector Routing Protocols. In Symposium on Network and Distributed Systems Security (NDSS'97), February 1997.

[20] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In Security Protocols, 7th International Workshop, edited by B. Christianson, B. Crispo, and M. Roe. Springer Verlag Berlin Heidelberg, 1999.

[21] Richard vonMises. U¨ ber Aufteilungs- und Besetzungswahrscheinlichkeiten. Revue de la Facult´e des Sciences de l'Universit´e d'Istanbul, 4:145—163, 1939.

[22] Seung Yi, Prasad Naldurg, and Robin Kravets. Security-Aware Ad-Hoc Routing for Wireless Networks. Technical Report UIUCDCS-R-2001-2241, Department of Computer Science, University of Illinois at Urbana-Champaign, August 2001.