Identification of Malicious Nodes Based on Node Grouping

[1]Aishwarya. S, [2]Mahalakshmi. J, [3]Ashok. P
[1]Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamilnadu, India

[2] Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamilnadu, India

[3]Assistant Professor, Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamilnadu, India

ABSTRACT

Here, malicious node identification methods against false notification attacks in MANETs using node grouping is proposed. Inhis method, the network formation occurs and many clusters are formed. Based on the highest delivery factor, the cluster head is formed through which the data transmission takes place from source node to the destination node. AODV protocol is used for routing. This does not have any detection mechanism, but the node can get the required route only on the demand. The source gets all route information concerning the nodes on the route. In the proposed methods, only the cluster head is involved in transmission, resulting in reduced delay, reduced communication traffic volume and increased packet delivery ratio.

Keyword:- *Ad hoc networks, cluster head, data verification request, malicious node.*

1. INTRODUCTION

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. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

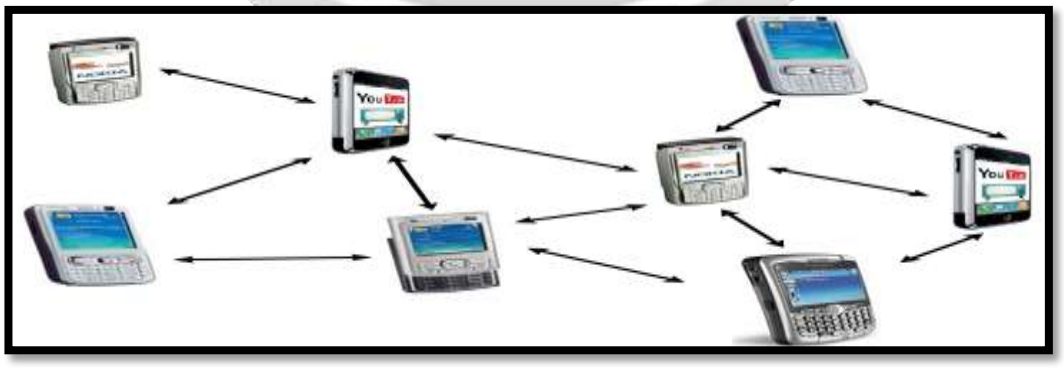

Fig -1: Mobile ad-hoc networks

A mobie ad-hoc network (MANET) is a multi-hop ad-hoc wireless network where nodes can move in an arbitrary manner in the topology. Therefore, the network may experience rapid and unpredictable topology changes. Such networks have no given infrastructure; can be set up quickly in any environment and generally are likely composed of nodes with constrained capabilities (power level, processing capacity, and so forth). Moreover, this kind of network could be linked to other infrastructure networks constituting a mesh network.

In MANETs, each node has poor resources (i.e., the communication bandwidth and the battery life of mobile nodes are limited). On the other hand, in MANETs, if a normal node becomes malicious owing to an attack from outside the network, the malicious node tries to disrupt the operations of the system. In this case, the user whose network contains the malicious node will typically continue to operate the system normally, unaware of the threat, while the malicious node may execute a variety of attacks. Malicious node can either perform Data Replacement Attack(DRA) or False Notification Attack(FNA) and sometimes both.

2. RELATED WORK

In this section, we review existing studies on secure routing and reputation systems.

2.1 Secured Routing

In the field of MANET, secure routing protocols protect against false notification of data and DoS attacks have been well studied. Secure routing protocols commonly employ data transmission along multiple routes (from the source node to the destination node) and data encryption using symmetric or public. The authors have proposed a method in which the source node determines multiple safe routes (from the source node to the destination node) by encrypting the route request message using a hash function before sending data items. However, the methods did not protect against malicious node attack, and thus cannot be directly applied to the problem addressed in this paper. The authors have proposed a method in which each sensor node sends data items with message authentication code (*MAC*), which are encrypted by using a symmetric key. When each node receives the message, it confirms the validity of the message by checking whether the received *MAC* is same as the *MAC* which is calculated from the received data items encrypted by the symmetric key. However, even if data items are encrypted, attacks described above cannot be avoided by these methods, because malicious nodes merely replace received data items with data items of their own.

2.2 Reputation Systems

In the distributed systems where there are malicious nodes or failure nodes, reputation systems, which evaluate the performance of nodes to exclude the malicious nodes from the network, have been widely discussed. In the field of sensor networks and MANETs, many reputation systems considering the reliability of nodes in the network have been proposed. Each node calculates the local reputation scores of other nodes from correctness of received files, and floods the score information in the network. Then, each node calculates the global reputation score from its own and received local scores. At last, it determines the node whose global score is lower than a threshold as the malicious nodes. The authors have proposed methods in which each node manages the reputation values of its neighboring nodes in MANET. In these methods, each node overhears messages sent by neighboring nodes and determines the reputation score of neighboring nodes by analyzing their messages.

However, these methods do not assume that the malicious nodes send false reputation scores. The authors have proposed methods against false notification attacks in reputation systems. Source nodes exchange a cryptographic key with destination nodes in advance, and send their own ID, along with the past and current reputation scores of destination nodes, in encrypted form. The destination node decodes and confirms the received reputation scores. Thus, it can discard the false reputation scores. However, these methods assume information sharing only between source and destination nodes, whereas in our method cluster head is created in each group based on the highest score which acts as the intermediate between source and destination.

3. MALICIOUS NODE IDENTIFICATION

3.1 Node grouping

The Network formation occurs and cluster groups are formed based on the neighbor availability and location of

nodes. Based on the highest delivery factor, the cluster head is chosen. This is followed by advertisement of cluster head which is broadcasted to all nodes in the network. Ad-hoc On demand Distance Vector routing protocol is followed. This protocol does not have any detection mechanism but the source node will have all the information concerning all nodes in the network.

In this process, the cluster head is alone involved in the transmission. Once the cluster head is chosen, it acts as the intermediate between the source node and the destination node. If the destination node is present within the same cluster, the cluster head directly communicates with the destination. If the destination node is present in a different cluster, the cluster head will communicate with the adjacent cluster heads until it finds the destination node.

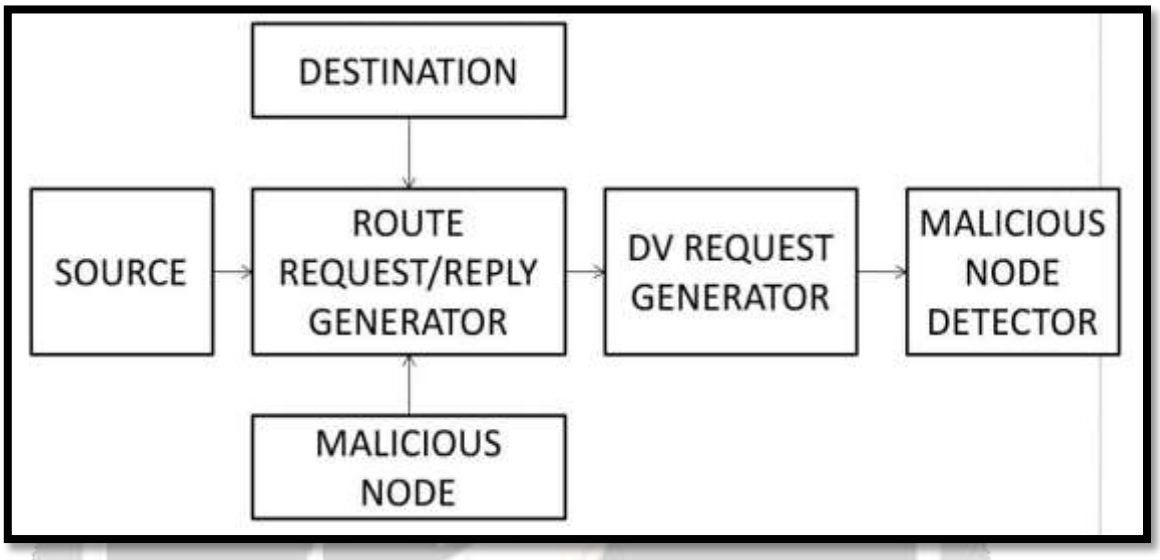

Fig -2: Block diagram

3.2 Detection of Malicious Node

Topology issues have received more and more attentions in mobile ad-hoc Networks (MANET). Most of the schemes have proven to be able to provide a better network monitoring and communication performance with prolonged system lifetime. The coverage topology describes the topology of sensor coverage and is concerned about how to maximize a reliable sensing area while consuming less power. The connectivity topology on the other hand is more concern more about network connectivity and emphasizes the message retrieval and delivery in the network. After selecting the destination, the source wants to send the data to the destination. So route has to be established for data forwarding. If the source has no direct route to the destination, then the source will initiate the route discovery in an on-demand fashion. RREQ is generated in source node and it is passed to all the intermediate nodes till it reaches the destination. Destination will reply with RREP to the source node via the route travelled by RREQ. With the help of RREP, source node will update the routing table and best route will be selected for data transmission.

After creating a network, a malicious node is included. Hacker nodes will always try to enter the network. Initially source will send Route Request(RREQ). Destination node will send a Route Reply(RREP). But, if any malicious node is present, it will send a fake Route Reply. Previous techniques can't check whether it is a fake route reply or not. Hence, the malicious node on joining the network will start to lose the data. The source and the destination nodes are initialized in the network.

Now, the route request RREQ is sent to destination node by the source node via the multiple nodes in multiple paths available in the network. Before it reaches the destination, the RREQ reaches the malicious node which is nearer to the source node when compared to that of destination node. So the malicious node replies to the source node by sending RREP. Hence there is an attack in the network. Then before the source's RREQ reaches the destination node the reply is sent to the source node by the malicious node, which restricts the source node from

further sending RREQ to the destination node.

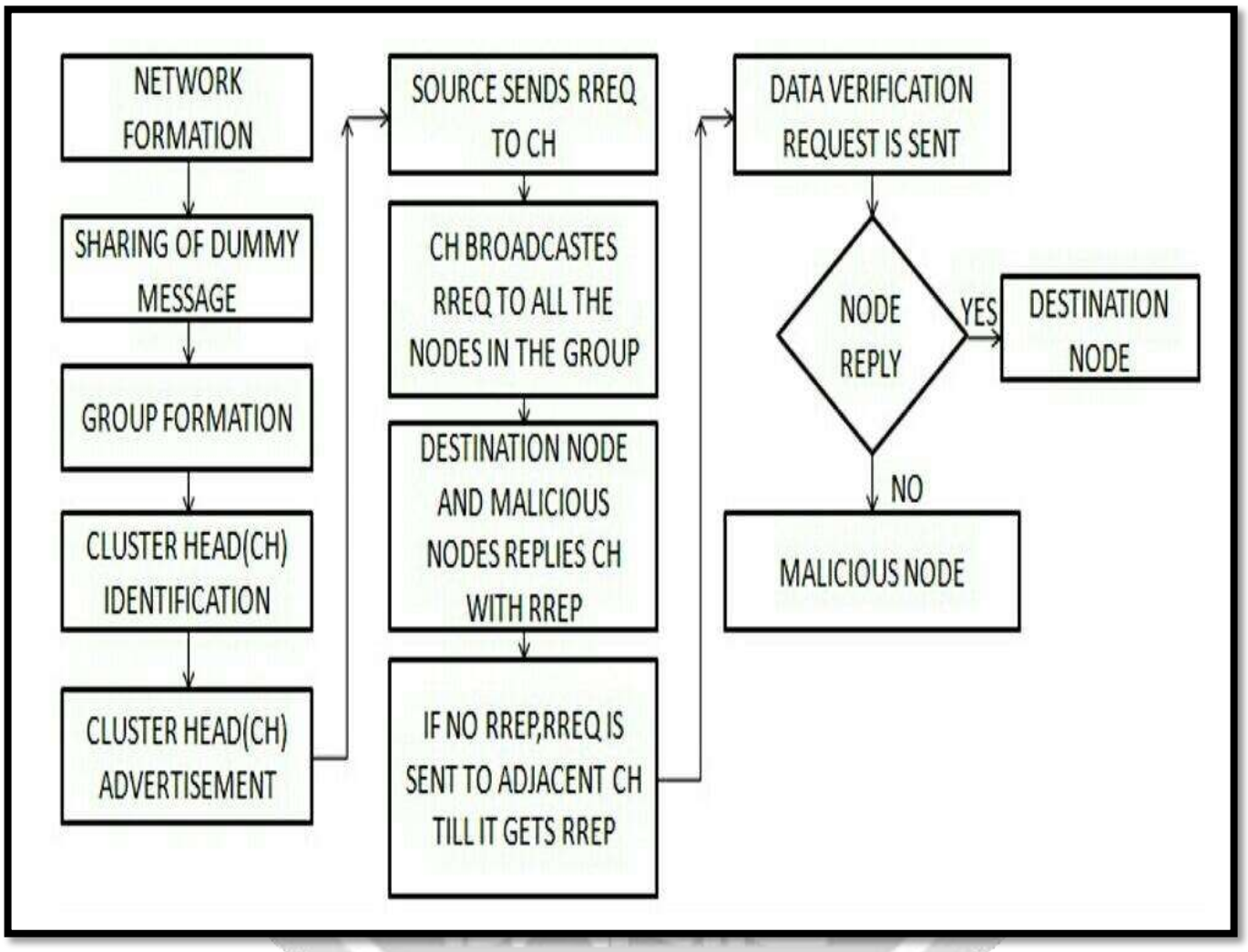

Fig -3: Flowchart for malicious nodes identification

To avoid this attack we go for node grouping to identify the malicious node in the network. A group is formed by issuing a dummy message and the cluster head is advertised. Now, the route request RREQ is sent to destination node by the source node via the cluster heads available in the network. The RREQ reaches the malicious node which is nearer to the source node when compared to that of destination node. So the malicious node replies to the source node by sending RREP.

In order to verify whether the node that sent the reply is malicious or the destination, the source node sends data verification request to all the nodes that send the RREP. The data verification request can only be replied by the destination node. The destination node thus replies for the data verification request which ensures that the data must be sent to that particular node. After verifying the destination node, the source node transmits the data to the destination node. Thus the malicious node can be easily identified.

4. RESULTS

The amount of energy saved in this system is higher than the normal system. It approximately amounts to about 5% to 7%. The number of packets delivered is more compared to the existing system. This increases the packet

delivery ratio. Normally all the nodes are involved in the data transmission. But here a cluster head is formed which is used for transmitting data from one node to the other. Since only a cluster head is involved in the transmission of data from source to the destination, there is the decrease in the delay as compared to that of existing system.

5. CONCLUSION

In this system, the methods for top-k query processing and malicious node identification based on node grouping in MANETs is proposed. In order to maintain high accuracy of the query result and detect attacks, nodes reply with k data items with the highest score along multiple routes. After detecting attacks, the query-issuing node narrows down malicious node and then tries to identify the malicious nodes through message exchanges with other nodes. When multiple malicious nodes are present, the query issuing node may not be able to identify all malicious nodes at a single query. It is effective for node to share the information about the identified malicious nodes with other nodes. In our method, each node divides all nodes into some groups by using the similarity of the information about the identified malicious nodes. Then, it identifies malicious nodes based on the information on the groups. In this system, the issue of identification of liar nodes (LNs) is not addressed. The future enhancement is to design a method to identify LNs, and also to design a message authentication method to prevent malicious nodes from performing FNAs.

6. REFERENCES

[1] Amagata. D, Sasaki. Y, Hara. T, and Nishio. S, 'A robust routing method for top-k queries in mobile ad hoc networks,' in Proc. MDM, Jun. 2013, pp. 251–256

[2] Balke.W.T, Nejdl. W, Siberski. W, and Thaden. U, 'Progressive distributed top-k retrieval in peer-to-peer networks,' in Proc. ICDE, Apr. 2005, pp. 174-185.

[3] Hu.Y.C, Johnson. D. B, and Perrig.A, 'SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,' Ad Hoc Netw., vol. 1, no. 1, pp. 175–192, Jul. 2003.

[4] Kurosawa. S, Nakayama. H, Kato. N, Jamalipour. A, and Nemoto. Y, 'Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method,' Int. J. Netw. Secur., vol. 5, no. 3, pp. 338–346, 2007.

[5] Liu. K, Deng. J, Varshney. P.K, and Balakrishnan. K, 'An acknowledgment based approach for the detection of routing misbehavior in MANETs,' IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[6] Sasaki. Y, Hagihara. R, Hara. T, Shinohara. M, and Nishio. S, 'A top-k query method by estimating score distribution in mobile ad hoc networks,' in Proc. DMWPC, Apr. 2010, pp. 944–949.

[7] Sasaki. Y, Hara. T and Nishio. S, 'Two-phase top-k query processing in mobile ad hoc networks,' in Proc. NBiS, Sep. 2011, pp. 42–49.