Cluster Based MANET of Self Node Detection in SCF+ Tree

[1]Nageswaran.C.M, [2]Faizal Mukthar Hussain.S

[1]PG Scholar, Department of Computer Science and Engineering, Mohamed Sathak Engineering College, Ramanathapuram, India.
[2]Assistant professor, Department of Computer Science and Engineering, Mohamed Sathak Engineering College, Ramanathapuram,India
[1]nages.cmp@gmail.com, [2]faizaldwyc@gmail.com

Abstract: Mobile Adhoc network (MANET) consists of various mobile nodes connected by wireless links. Security and congestion control is the essential problem in ad-hoc networks. Congestion control is correlate to regulating traffic incoming into a telecommunication network. The security and congestion in MANET leads to many problems such as wormhole attack, DoS, Long delay, many packet calamity, and high aerial. In MANET, nodes can fully move around while communicating with each other. A node may be start working selfishly by using its limited resource only for its individual benefit such selfish node and wormhole attack problems for a MANET. Multiple path is selected with the advice of Multicast Ad-hoc on demand distance vector (MAODV) routing protocol. The watchdog node watches the behavior of each node. If any node misbehaves or initiate wormhole attack, it will apprise to the path rater. The path rater will decide to remove the selfish node or wormhole attack. It takes redundant amount of time to identify the selfish node such as the wormhole attack and does not properly identify the misbehaving nodes so it leads to the packet dropping. To overcome these issues, SCF+ tree construction is proposed to identify wormhole attack and remove the selfish node.

Index Terms— MANET, MAODV, Path rater, Wormhole attack, SCF+ tree construction

1. INTRODUCTION

A "mobile ad hoc network" (MANET) consists of various mobile nodes connected by wireless links. The union of which makes an arbitrary graph. In a MANET, nodes can openly move around while communicating with each other .There are two types of MANETs: open and closed. These networks build and start with the help of constituent wireless nodes. Since these nodes have only a limited transmission range, it depends on its neighboring nodes to progressive packets. A node may be start working selfishly by using its limited resource only for its individual benefit; such nodes selfish cause a wide range of problems for a MANET[1].

MANET is a collection of self-governing nodes that communicate with each other by forming a multi-hop network and maintaining connectivity in a decentralized manner, MANET is decentralized, self-organizing networks which make a point to point communication in between source and destination from a suitable route in the presence of any one routing protocol like AODV, GRP (Gathering based routing protocol), DSR (Dynamic Source Routing), OLSR (Optimized Link State Routing), TORA etc. Some well-known Applications of Mobile Ad Hoc Network are following:

- Military: Automated battlefield, Special operations, Homeland defence.
- Civilian: Disaster Recovery (flood, fire, earthquakes etc), Law enforcement (crowd control), Search and rescue in remote areas, Environment monitoring (sensors), Space/planet exploration.
- Commercial: Sport events, festivals, conventions, Patient monitoring, Ad hoc collaborative computing, Bluetooth, Sensors on cars (car navigation safety).

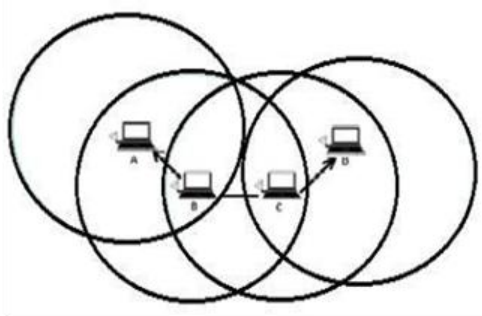


Figure.1: Mobile Ad-hoc Network

Whenever a communication is stable between

source and destination, then destination node should be lie in between the radio range of the source node which wants to initiate the communication.

This mobility causes frequent network partitions hence data accessibility in ad hoc networks is lower than the fixed networks. The nodes which are not willing to forward packets and share their memory space are called selfish nodes. The selfish node that does not allocate data items for the purpose of other nodes is called selfish node and routing can be disturbed when routing control messages are tunneled[5],[6]. This tunnel between two colliding attackers is referred as a wormhole. External attackers arise in network from the outside boundaries of network and attempt to interrupt the network by injecting invalid routing information. They create routing loops or other non-functional routes and try to partition. So, these attacks can degrade the performance of network.

2. RELATED WORK

The logic behind clustering is to group the network nodes into a number of overlapping clusters. Inside the cluster one node that coordinates the cluster activities is cluster head (CH). In the present architecture, the MANET area has been split into a number of size clusters having cluster head and storage capability according to bandwidth, connectivity degree, RSS (relative signal strength) as per the cluster formation algorithm given. To create the cluster in MANET, take two strong parameters connectivity degree of nodes and RSS (relative signal strength among nodes) on the basis of these parameters clusters form in MANET.

The cluster head is decided according to the maximum connectivity degree of a node. The main function of watchdog is to detect misbehaving node and wormhole attack. this method is that it detects failures not only at link level but also at the forwarding level , This algorithm works with AODV (Ad hoc on demand distance vector) routing protocol[8]. After finding the misbehave node and selfish node, the node is removed from the path using path_rater. Path_rater decides the route of packets from one node to another in a MANET[10]. Path_rater uses knowledge of misbehaving nodes reported by watchdog. The exact path the packet has traversed has to be known by path_rater hence it should be implemented on top of source routing protocol. After removing false node a new path is called by AODV.

3. PROPOSED SYSTEM

To overcome the problems present in the existing system, propose the new methods such as MAODV algorithm and SCF+ tree. Wormhole attack occurred due to some malicious node present in network. In this paper, new scheme is used to detect and remove malicious nodes and selfish node from network. This scheme initially introduces SCF+ tree in network.

The proposed strategies are inspired by the real-world observations in economics in terms of credit risk and in human friendship management in terms of choosing one‟s friends completely at one‟s own discretion .Then applied the notion of credit risk from economics to detect selfish nodes and wormhole attack. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness. Since AODV techniques failed to consider selfish nodes and wormhole attack, also proposed MAODV techniques.

The selfish node and wormhole attack are detected by the self-replica allocation. They are based on the approach of a self-centered friendship tree (SCF+ tree) and its variation to achieve high data accessibility with low communication cost in the presence of selfish nodes and misbehaving mode. With the measured degree of selfishness, SCF-tree models human friendship management in the real world. The key feature of the SCF-tree-based replica allocation techniques is that it can minimize the communication cost, while conclude high data accessibility. Here each node detects selfishness and wormhole attacks, without forming any group or engaging in lengthy negotiations.

The main goal of this project is,

- It reduces the time consumption
- This concept does not make the packet dropping
- It reduces the wormhole attack and forwarding data to destination node.

3.1Node formation

In MANETs, every node acts as a router and communicates with each other nodes. If the source and the destination mobile hosts are not in the coverage area, data packets are forwarded to the destination host through other nodes which exist between the two mobile hosts. MANETs does not require any infrastructure and base station. MANETs are applicable

in many situations such as battlefield and disaster area. In ad hoc network, as all the nodes are having mobility and can move freely. This mobility causes frequent network partitions hence data accessibility in ad hoc networks is lower than the fixed networks.

First the node is formed to transmit and also receive the packets in the MANET. Here, set more number of nodes for clustering, sending and receiving the packets from sender to receiver. Then 200 nodes are formed for processing. The node formation is the first step of process in which nodes are added in to the network. The nodes are in mobile nature and are free to move.

3.2 Clustering

The Next process is to clustering the nodes. In clustering process is grouping the moving nodes. The moving nodes are grouped and again it can be moved to some other locations. Clustering procedure, a representative of each sub domain (cluster) is „elected" as a cluster head and a node which serves as intermediate for inter-cluster communication is called gateway and the resting members are called ordinary nodes.

The boundaries of a cluster are defined by the transmission area of its CH. With an underlying cluster structure, non-ordinary nodes play the role of dominant forwarding nodes. The logic behind clustering is to collect the network nodes into a number of overlapping clusters. Clustering makes possible a hierarchical routing in which paths are recorded between clusters instead of between nodes. Inside the cluster one node that manages the cluster activities is cluster head. Inside the cluster, there are ordinary nodes also that have direct access only to this one cluster head and gateway.

Gateways are nodes that can hear two or more cluster heads. Ordinary nodes send the packets to their cluster head that either distributes the packets inside the cluster, or the destination is outside the cluster then forwards them to a gateway node to be delivered to the other clusters. According to the movement of the nodes it can be grouped with every node in the network. The newly created grouping details are updated in the network. Here, the cluster head can be selected with the help of some parameters. There are node connectivity, Degree of nodes and RSSI value.

3.3 Path selection

MAODV implementations have two key limitations: 1) Only group members can send multicast traffic to the multicast group 2) The multicast data packets are unicast, resulting in wasted bandwidth. Each multicast group has a unique multicast group address. According to the MAODV stipulation, each multicast group is formulated by using a tree structure, composed of the group members and certain routers, which are not group member but must exist in the tree to connect the group members. The group members and the routers are all tree members and belong to the group tree. Linked with each multicast tree, the group member that first establishes the tree is the group leader and authority for maintaining the group tree by periodically broadcasting Group-Hello (GRPH) messages in the whole network.

Each node in the network may maintain three tables such as Unicast Route Table, reporting the next hop for routes to other destinations for unicast traffic. A special case is when the destination is a multicast address, which presents when the node is not a multicast tree member but has multicast data packets to send to that multicast group. The second one is Multicast Route Table; classify the next hops for the tree structure of each multicast group. Each entry performs one group tree structure and every node belongs to that group tree should maintain such entries with its own identity as group leader or router.

Every next bound is linked with direction either downstream or upstream. If the next bound is one-hop nearer to the group leader, the path is upstream otherwise it is downstream. The group leader has no upstream but other nodes in the tree should have one and only one upstream. The third table is Group leader table and it records the currently-known multicast group address with its group leader address and the next hop towards that group leader when a node receives a periodic GRPH message. It also combines the function of the request table.

MAODV implementation supports that every node in the network can send out multicast traffic, must consider how these data packets reach each multicast group member if the data source node is not a tree member. Choose a two-step ways: first step, there is a route from that data source node to a tree member; then after the tree member receives the multicast data packets, it generates the data through the whole tree, reaching every group member. After clustering the nodes in the mesh network need to choose the source and destination. Then choose the path for sending packets to the destination. For that purpose, MAODV is used for transmitting the packets between the source

and destination. Then multicast tree is established when a sender wants to send data to many receivers. A MAODV protocol can select the best path from source to destination.

3.4 False node detection

Nodes are not forward the other packets, thus it maximizing their benefits at the expense of all others. Nodes are failing hardware or incorrect software. Do not intentionally misbehave but if impair the working of the net, and then have to be treated just as malevolent or selfish nodes. The node does not respond to route request messages. This is a selfish behavior but it does not impair the net as it will find another route. The node on its own it is perfectly rational to avoid the selfish node and increase its own throughput but for the net at large this is a bad choice as it does not punish the selfish node but only burdens the cooperating ones with more work.

A selfish Node degrades efficiency of packet transfer and accelerates the packet delivery time and packet loss rate and finally creates Network Partitioning. Node leveling technique that takes into account integrated degree of selfishness. During replica allocations, a node regards all connected nodes as its friends. Consequently, the proposed replica allocation strategy can utilize all connected nodes, including selfish nodes as well as non-selfish nodes.

Route maintenance is used to handle link break and if a node detect there is a link break from data link layer, it will generate a RERR packet and send back to the source node using the part of the route traversed so far. The reveal source node must delete the broken link from its route cache table. If the source node has another packet to send to the same destination, it must try addition route or invoke route discovery process again if it does not have any other routes.

The main portion is to detect the false nodes in the network so SCF+ tree construction is used. According to that, easily find the offend nodes and wormhole attack in the MANET. Using SCF+ tree, detect the node behavior as normal or abnormal, here the request will be send to next node. According to the request, the misbehaving node can be detected. If the node sends any replicas to one request, the behavior of node can be monitored.

4. SYSTEM FLOW DIAGRAM

The overall system design shows that the node is formed to transmit and also receive the packets in the MANET. Set more number of nodes for clustering, sending and receiving the packets from sender to receiver and number of nodes are formed for processing.

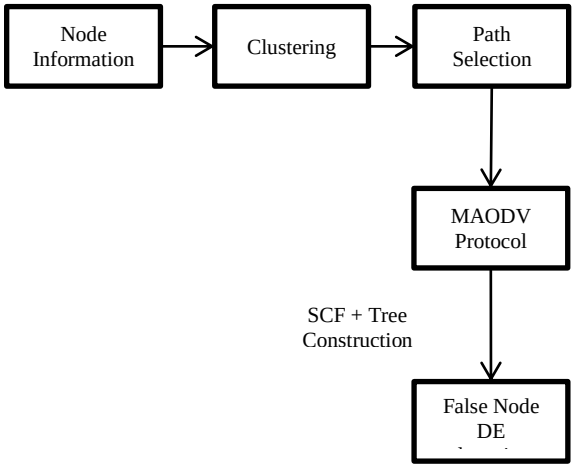
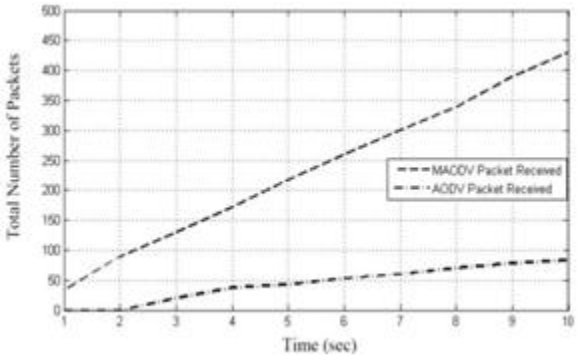


Figure2: System flow diagram

In the process of node formation, nodes are added in to the network. The nodes are in mobile nature and are free to move. Then clustering is formed which means grouping the moving nodes. The moving nodes are grouped and again it can be moved to some other locations after that the efficient path is selected sending packets to the destination by the use of MAODV routing protocol. The path may contain false node and wormhole attack which is identified and removed by SCF+ tree construction.

5. PERFORMANCE EVALUATION



Figuere 3: Total Number of Packets Received

These metrics shows the total number of Packet Received at output in the case of wormhole attack with

AODV and without wormhole attack or MAODV. If malicious node is occurred in network then packet received is decreased in the case of MAODV and output maintain as input.

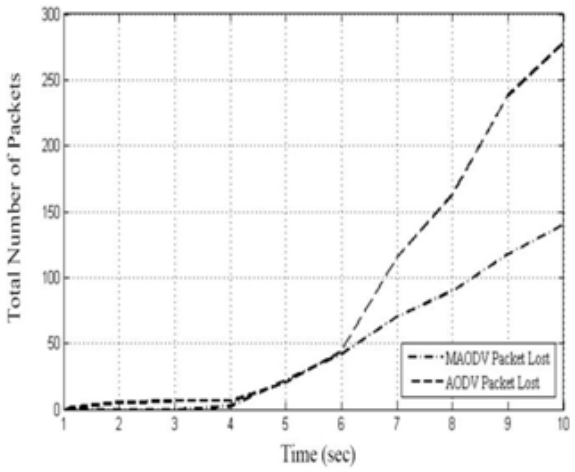


Figure 4: Total Number of Packets Dropped

The metrics shows that the total number of packet dropped in the network. Data dropped is increases by increasing the malicious nodes in network, as a result of consistently failing of data packets. The evaluation result shows the output of both with and without (MAODV) wormhole attack.

Figure shows the packet drop in MANET, it clarify that there is less number of packet drop is occurred in MAODV as compare to AODV with wormhole attack and the numeric value is further evaluated.

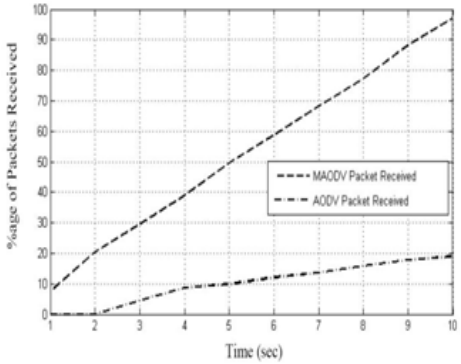


Figure 5: Packet Delivery Ratio

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

In an adhoc network, the transmission range of nodes is limited; hence nodes mutually cooperate with its neighboring nodes in order to extend the overall communication. MAODV routing protocol is proposed in this concept, it will choose the shortest and also the efficient path between the source and destination. This MAODV protocol avoids the packet loss in the network during the identification of false node and wormhole attack. Then the SCF+ tree construction is used to identify the misbehaving nodes and wormhole attack presented in the network.

Novel node leveling technique is also proposed that utilizes the memory space of all connected nodes, including selfish nodes and wormhole attacks as well. The experimental results show that the proposed system can efficiently handle the system resources and improve the system flexibility and reduced the system cost.

6.2 Future work

In this concept, identify the selfish node with the help of the SCF+ tree algorithm. Mobile agent is used in future. The main aim of this mobile agent is to identify the misbehaving such as selfish node. The process of mobile agent is as follows: A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding. Every node has a unique id in the network, which is assigned to a new node collective by existing nodes. The source node generates mobile agent after a specific period of time. The mobile agent moves towards forward path created using RREQ and RREP. The agent calculates the packet receive and forward by a node. If the agent discovers a malicious node, rather than moving forward, it sends a report to the source node.

7. ACKNOWLEDGEMENTS

Words are inadequate in offering thanks to the respective Head of the Institution, Head of the Department and Faculty members for giving valuable advice, guidance, monitoring and constant encouragement for technical support.

REFERENCES

[1] Gaurav, Naresh Sharma Himanshu Tyagi," An Approach: False Node Detection Algorithm in Cluster Based MANET," Volume 4, Issue 2, February 2014.

[2] Duc A. Tran, Member, IEEE, and Harish Raghavendra, "Congestion Adaptive Routing in Mobile Ad Hoc Networks", IEEE Transactions On Parallel and Distributed Systems, Vol. 17, No. 11, November 2006.

[3] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog", IEEE Communications Letters, Vol. 16, No. 5, May 2012.

[4] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu, Fellow, IEEE, "Handling Selfishness in Replica Allocation Over a Mobile Ad Hoc Network", IEEE Transactions on Mobile Computing, Vol. 11, No. 2, February 2012.

[5] Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, TWOACK: "Preventing Selfishness in Mobile Ad Hoc Networks", 0-7803-8966-2/05/$20.00 (C) 2005 IEEE.

[6] Vishnu Kumar Sharma1 and Dr. Sarita Singh Bhadauria2,"mobile agent based congestion control using AODV routing protocol technique for Mobile ad-hoc network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012.

[7] G. Cao, L. Yin, C.R. Das, "Cooperative cache-based data access in ad hoc networks", IEEE Computer 37 (2) (2004) 32–39.

[8] Yang Zhang, Student Member, IEEE, Liangzhong Yin, Jing Zhao, and Guohong Cao, Fellow, IEEE, "Balancing the Tradeoffs between Query Delay and Data Availability in MANETs", IEEE Transactions On Parallel And Distributed Systems.

[9] T. Hara and S.K. Madria, "Data Replication for Improving Data Accessibility in Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1515-1532, Nov. 2006.

[10] P. Padmanabhan, L. Gruenwald, A. Vallur, and M. Atiquzzaman, "A Survey of Data Replication Techniques for Mobile Ad Hoc Network Databases," The Int‟l J. Very Large Data Bases, vol. 17, no. 5, pp. 1143-1164, 2008.

[11] T. Hara and S.K. Madria, "Consistency Management Strategies for Data Replication in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 8, no. 7, pp. 950-967, July 2009.

[12] M. Tamilarasi and T. Sundararajan, \Secure enhancement scheme for detectingsel_sh nodes in manet," pp. 15, 2012.

[13] S. Singh, P. Jain, P. Bindra, and C. Goel, \Opnet based simulation and perfor-mance analysis of aodv and grp by varying number of misbehavior nodes."

[14] T. Lacey, R. Mills, B. Mullins, R. Raines, M. Oxley, and S. Rogers, Ripsec{usingreputation-based multilayer security to protect manets," Computers & Security,2011.

[15] A. Ajina, G.R. shaktidhrma,\study of energy efficient, power aware routingalgorithm and their applications.2010 second international conference on machine learning and computing.

[16] S.Usha, S.Radha\ a collective network arbitration protocol to detect mac misbehavior inmanets2010.

[17] Md.Sharma, M.Inamullah\ Misbehavior detection in mobile ad hoc networksusing Artificial Immune System approach 2011.

[18] F.Xing, W.Wang\ on the survivability of wireless ad hoc Networks with node misbehaviors and failuresieee transactions on dependable and secure computing, vol. 7, no. 3, july-september 2010.

[19] K.Vats, M. Sachdeva, K.Saluja,\Simulation and performance analysis of olsr routing protocol using opnet volume 2, issue 2 feb 2012.

[20] Q Li, G.Cao\ mitigating routing misbehavior in disruption tolerant networks ieee transactions on information forensics and security, vol. 7, no. 2, april 2012.

[21] S.agrwal, S.Jain, S.Sharma\ Mobility based performance analysis of aodv and dymo under varying degree of node misbehaviour. Volume 30-No.7,Sep2012.

[22] Ratish Agarwal, Dr. Mahesh Motwani, Survey of clustering algorithms for MANET, Ratish Agarwal et al / International Journal on Computer Science and Engineering Vol.1 (2), 2009, 98-104.

[23] I. Er and W. Seah. "Mobility-based -hop clustering algorithm for mobile ad hoc networks". IEEE Wireless Communications and Networking Conference Vol. 4. pp. 2359-2364, 2004.

[24] P. Basu, N. Khan, and T. D. C. Little, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks," in proceedings of IEEE ICDCSW‟ 01, pp. 413–18, Apr. 2001.

[25] Ms. I.Shanthi and Mrs. D. Sorna Shanthi, "Detection of false alarm in handling of selfish nodes in MANET with congestion control", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 3, January 2013 ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814.