M-CONFIDANT: A Multicast based Cooperation of Node Fairness in Dynamic Ad hoc Network

Sarvesh Acharya
Student, LFTS
Lovely Professional University
Jalandhar, INDIA

Gulshan Kumar
Assistant Professor
Lovely Professional University
Jalandhar, INDIA

Vikas Singh
Student, LFTS
Lovely Professional University
Jalandhar, INDIA

ABSTRACT
Mobile Ad-hoc Network (MANET) consists of many wireless mobile nodes that temporally constitute a dynamic infrastructure less network. To enable communication between nodes that do not have direct contact, each node must function as a wireless access point and potentially forward data traffic on behalf of the other nodes present in the network. Due to limitation of resources with these Mobile nodes the property of selfishness is exhibited. A technique system level based Cooperation of Node Fairness in Dynamic Ad hoc Network that promise to detect and nullify the effect of selfish nodes on the basis of monitoring, assigning reputation measure to every node and isolation of the detected misbehaving nodes. Previously, this scheme was implemented in GloMoSim simulator using unicast protocol and the idea is to integrate the CONFIDANT protocol with multicast protocol, so that the network performance can be boosted.
In this paper, we suggest a M-CONFIDANT: A Multicast based Cooperation of Node Fairness in Dynamic Ad hoc Network. This scheme integrates a multicast based MAODV protocol with the CONFDIANT protocol previously integrated with DSR protocol.

General Terms
CONFIDANT, MAODV, DSR, mobile ad hoc network

Keywords
Routing, cooperation, reputation, mobile ad-hoc networks, multicasting

1. INTRODUCTION
Mobile Ad hoc NETwork(MANET) is formation of the network in which the nodes are not positional stable and roam across the network. To extend the reach ability of a node, the nodes act themselves as routers. MANET is a self-configuring infrastructure less network of mobile devices connected by wireless medium. The following subsections describe the multicasting in ad hoc network and the integration of CONFIDANT scheme with the multicast protocol.

1.1 Broadcasting Approaches in MANET:
There broadcasting approaches are classified on the basis of cardinality of destination:
- Unicasting: Communication between a single source to a single destination.
- Multicasting: Communication between a single source to a multiple destinations.
- Broadcasting: Flooding of messages to all the destination nodes.
- Geocasting: Communication between a source to all nodes inside a geographical region.

1.2 Multicasting in Ad hoc Routing
Various application supports has been enabled with the introduction of multicast data routing such as video conferencing, video streaming and distance learning. Transmission of the data to a group of destination nodes from a single source node constitutes the main benefit of multicasting by significantly reducing the network load where packets are needed to be transmitted to a group of nodes. However, dynamic topology and bandwidth constraints in MANET environment, pose great challenge to the multicast routing protocol. The various suggested routing protocols are classified into following two categories, Tree Based follows the formation of tree infrastructure in which source node acts as root node and only a single path between the two communicating nodes. Mesh Based provides multiple routes between the communicating nodes. These protocols are more robust than the tree based. Following are the various multicast routing protocols:
- Multicast ad hoc on-demand distance vector (MAODV)
- Amris: a multicast protocol for ad hoc wireless
- Amroute: ad hoc multicast routing protocol
- On-demand multicast routing protocol (ODMRP)
- Fatnemo: Building a resilient multi-source multicast fat-tree.
- PUMA

1.3 Packet dropping
Intermediates nodes that may exhibit malicious or selfish behavior and packet can be dropped based on frequency and selectiveness as mentioned below:
- Selective Dropping
- Constant Dropping
- Periodic Dropping
- Random Dropping
- Repeater Attack

The packet dropping results in large drop in performances of the network and the network won't be able to operate efficiently and effectively. In this attack, a malicious node I simply replays packets of one of its neighbor A. This will result in other side neighbor (say one of them is B) assuming that the A is its neighbor, in fact it is not. Two nodes are said to be neighbor if they are in transmission range of each other. Now the malicious node I can selectively replay packets between A and B, while dropping other packets. This would cause a Denial of Service for the nodes A and B. This scenario is difficult to detect as nodes can assume that this periodic dropping is because of noisy channel. Network services in mobile ad hoc network may be disrupted due to the

selfish behavior of the nodes. For the detection of selfish node behavior three categories of schemes are classified into three forms credit based scheme, reputation based scheme and acknowledgement based scheme. The reasons considered for this paper are limitation of resources:

- Packet drop due to bandwidth constraint: Mobile ad hoc network may have low capacity links established wireless network more susceptible to interference, external noise and signal attenuation effects which may lead to packet drop.

- Packet drop due to limited power supply: The mobile ad hoc network devices have limited resources available in terms of power supply. The devices may act reserved when it comes to the network participation to forward data packets from other nodes. In MANET nodes have to optimally use this resource.

- Packet losses due to transmission error: High bit error rate (BER) may be the reason for higher packet dropping in the ad hoc network. Increased collisions due to the presence of hidden terminals, presence of interference, location dependent contention, uni-directional links, frequent path breaks due to mobility of nodes, and the inherent fading properties of the wireless channel.

2. RELATED WORK

Yufang Zhu et al. implemented MAODV, multicast extension of AODV. MAODV is a tree-based routing protocol in which tree members are only allowed to communicate data packets debarring outsiders. MAODV is implemented in Network Simulator 2 (NS2). The results collected in the form of packet delivery ratio and latency indicate the encouraging results for less senders and low mobility while on increasing the senders and mobility the performance deteriorates.

A mesh-based protocol suggested by W. S. Yunjung et al. On-Demand Multicast Routing Protocol (ODMRP) uses the concept of forwarding group to construct a mesh between source and all of its receivers. By adopting mesh structure, ODMRP can achieve more reliable data delivery in case of node movements. However, it is not designed to support the multisource multicast efficiently.

Chia-Hui Huang et al. proposes a multisource scenario based MAODV protocol that is implemented with fast partition recovery scheme. This implementation scheme showcases the better results that avoid bottleneck problem. The recovery time has also been reduced as the recovery can be initiated without any permission.

Performance comparison of multicast protocols by Sung-Ju Lee et al., various routing multicasting protocols is classified on the basis of strengths, weaknesses and applicability.

Jayanta Biswas et al. present an efficient hybrid multicasting protocol based on ODMRP protocol due to the overheads incurred due to higher control overhead. This efficient protocol suits the high mobility and scalability issues of ODMRP protocol.

Ashok M. Kanthe et al. classifies packet drop attack as denial of service attack d**ue to the** bandwidth and memory buffer limitation, queue manager. A scheme based on reputation and trust mechanism to improve the network performance.

There are many of the suggested node cooperation enforcing schemes such as CORE, CONFIDANT, OCEAN, SORI and LARS [1][8][9][10][12]. CONFIDANT is the scheme that is chosen as the node cooperation. The following is the reputation system based scheme.

3. CURRENT SYSTEM

3.1 MAODV Routing Protocol

AODV is an ad hoc routing protocol for unicast traffic and MAODV a multicast extension to AODV for multicast traffic. [5][6] MAODV has two limitations:

- Multicast traffic can be sent by the group members to the group members only.
- MAODV allows the nodes to send multicast data packets that are broadcast while propagating along multicast group tree.

A unique group address is assigned to each multicast group that are organized by tree structure. The first node that constructs the tree is group leader for that tree. Group-Hello (GRPH) packets are broadcasted for network maintenance by group leader. For every node in the group the following three tables are maintained:

- Unicast Route Table – Next node is recorded for unicast traffic to the destination.
- Multicast Route Table – Multicast group's next node is recorded for tree structure. This entry is maintained by every node belonging to that group. Nodes are associated with direction downstream or upstream. The direction is upstream for the nodes one hop nearer to the group leader otherwise downstream while the group leader has no upstream.
- Group Leader Table – The currently-known multicast group address with the group leader is recorded.

Route Discovery and Maintenance For Reaching A Specific Node - Route discovery and Maintenance is the main task of AODV protocol. Detection of broken links is performed at MAC layer by using one-hop Neighbor-Hello.

Route Discovery And Maintenance For Reaching A Multicast Tree - There is a provision for every node in the network to send multicast traffic. The main issue is the reception of these packets by the nodes sent by the nodes outside the multicast group not member of tree. Firstly the packet is routed from source to a tree member then the data is propagated through the whole tree, reaching every node member of the tree.

The initial process of route discovery and maintenance accomplished as of existing mechanism in AODV using Unicast Routing Table. In MAODV source node has the information about the routing to group leader. Multicast data forwarding can be performed by nodes only if part multicast tree and uses Multicast Route Table otherwise it checks for Unicast Route Table.

Multicast Tree Construction - RREQ and RREP messages as of AODV are used for tree construction and MACT for the last step. A node before joining a multicast group creates an entry in its Multicast Route Table without an unknown group leader address and without upstream and downstream next hop and initiates with join flag (RREQ-J) of broadcast nature. A node has information about the group leader if it sends RREQ-J for the first time and is sent unicastly towards the group leader. The tree members with higher group sequence number can reply to RREQ-J with RREP-J.

Multicast Route Activation (MACT), a new message is used for grafting a branch to the tree. After sending RREQ-J node waits for specific RREP_WAIT_TIME time, if the RREP-J is already received and cached then it sends MACT-J towards the cached upstream and new next hop is added in Multicast Route Table. A node should add a new next hop downstream

for the every received MACT-J in its Multicast Routing Table and the tree branch is finally grafted.

For several sent RREQ_RETRIES to join a group tree and none received RREP-J means either the non-existence of group or the requesting source cannot reach that group due to network partition. This means that the source node becomes the first node of that group and thus the group leader that has to maintain the group sequence number and tree structure.

Multicast Tree Maintenance - Multicast tree maintenance is involves many processes in comparison to unicast route maintenance that are as follow:
Periodic Group-Hello Propagation
Group-Hello message (GRPH) must be broadcasted periodically throughout the network by group leader to indicate the existence and status of that group. The GRPH message received by the nodes leads to the updation of its Group Leader Table. In case the node not a tree member, it retransmits the first-time received GRPH. A GRPH message is transmitted from upstream to downstream that enables the updation of group sequence number, group leader and distance from the group leader of that node.

If a node receives a GRPH from its upstream and indicates the different group leader then there exists another group tree with same group address but with different leader and these trees can be connected. Then the trees can be merged and the tree merge process is initiated by the tree member with the smaller address indicated in the GRPH.

Neighbor Connectivity Maintenance - Neighbor connectivity maintenance of a link downstream is detected if broadcast messages are not received in a specific time. After detection, the downstream node removes next hop in Multicast Route Table and then sends out RREQ-J as a source node for new branch. The RREQ-J is sent with additional information about the hop count to the group leader to avoid the old branch. Update flag (GRPH-U) is sent to change its group information such as group leader, group sequence number or hop count to its group leader.

Group Leader Selection - Group leader selection process is initiated either for the existing group leader revokes its group membership or new group leader to be selected for the new partitioned tree. The current node with one downstream node cancels the entry for that group in its Multicast Route Table that indicates that it no longer is the member of that tree. MACT with prune flag (MACT-P) is sent to downstream node that indicates the revocation of its group membership and that the group needs a new leader. For more than one downstream node, it sends MACT with group-leader flag (MACT-GL) to that node in either of the direction. MACT-GL indicates that that the tree has more branches and a leader is required for the tree. On receiving MACT-P, the node removes its upstream link from its Multicast Route Table and on receiving MACT-GL the node changes its upstream direction to downstream.
Membership Revocation - Group membership can be revoked by any member of the group including group leader. A node whether group leader or node discards its membership by changing its identity to router. For a node having downstream node it must stay or the node can self-prune from the multicast tree.
Tree Merge - If a tree member with smaller group leader address receives a GRPH from group leader with larger aggress for the same group. The merging is performed by sending unicast RREQ with repair flag (RREQ-R) to its group leader. The node then requests for the permission from group leader for rebuilding the tree. Depending upon the permission granted or denied the process proceeds. A node starts Tree-rebuilding by sending unicast join-and-repair flag (RREQ-JR) to group leader with larger address. The group leader with larger address sends RREQ-JR downstream to the source, in case a non-member node receives, the node becomes router for the for the new tree. When a group leader with smaller address receives RREQ-JR, this group leader updates its downstream nodes to upstream node and changes its identity to group member and a new tree is built. GRPH-U towards downstream is sent by old group leader to indicate changes about the group information.

3.2 The CONFIDANT Protocol

Purposed in 2002 by Sonja Buchegger and Jean-Yves Le Boudec [1], Cooperation of Node Fairness in Dynamic Network (CONFIDENT) interacts with the misbehaving node in the network. Reputation System based CONFIDANT scheme for detection and isolation of misbehaved nodes from the network. As the detected misbehaved nodes cannot initiate the communication process until the reputation measure for the nodes is improved. Each node performs four components that are implemented with CONFIDANT. There is interaction between the components to process and provide protocol information. The protocol components interact as follows:

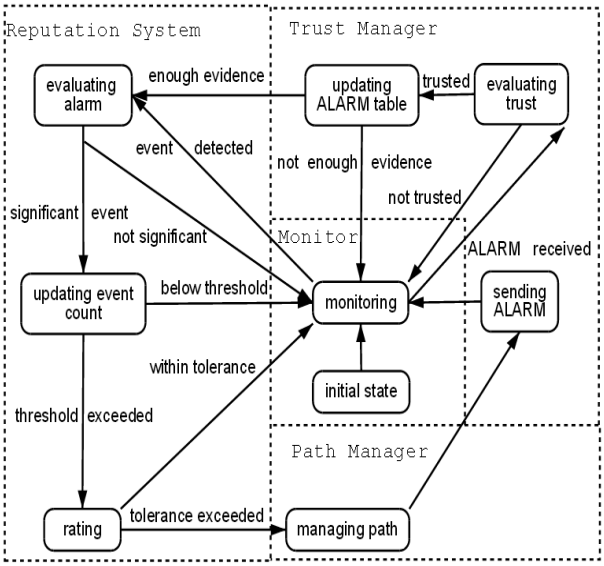

Figure 1 CONFIDANT Protocol [1]

- Monitor, the first-hand information is collected regarding the behavior of neighboring nodes achieved by observation and detection by passive acknowledgement. When a given misbehavior occurs, the reputation system is called. Message modification and fabrication are the other attacks that are part of monitoring process.
- Reputation system, Reputation system is responsible for the maintenance of reputation value of other nodes based on first-hand information obtained from the monitoring process and second-hand information.
- Trust manager**,** Trust manager has the task of maintaining the trust rating of the nodes.
- Path manager, after the information generated by trust manager about the nodes present on the network the processing is performed by path manager.

In CONFIDANT protocol, the monitor process involves the process of keeping an eye on its one-hop neighbours. Then

reputation system receives the information depending upon suspicion where the event is checked for the occurrence more than the pre-defined threshold and this constitutes the rating for the nodes in the network. Depending upon the rating ALARM message is generated and is sent to the suspicious node by trust manager component. ALARM message contains the information about the event occurred like:

- Type of protocol violation,
- Number of occurrences,
- Self-originated message by sender,
- Address of reporting node,
- Address of observed node and
- Destination address.

Monitor component passes such messages on to trust manager where the evaluation of the source is performed. Determination of the impact of CONFIDANT protocol on the performance metrics where the nodes of the network act maliciously is performed using the metrics such as Good put and Overhead.

4. PROPOSED SCHEME

To force the cooperation and fairness of the CONFIDANT scheme onto the multicast mobile ad hoc network and along with the robustness.

4.1 M-CONFIDANT

The ad hoc network for implementing CONFIDANT protocol as a part of multicast routing protocol is Multicast based AODV protocol. M-CONFIDANT is a multicast based CONFIDANT protocol. In multicast network like MAODV that is a tree based they have limited network i.e. the group with the same multicast group id to analyze so the nodes. In multicast network multiple nodes can communicate at a particular time so the network overhead can be reduced at a large scale. As in MAODV non-member communication is using unicast data packets, this saves from the network overhead that would be incurred for multicast packet. Mesh based approach sacrifices multicast efficiency in comparison to tree based approach.

So the choice for the multicast routing protocol is for MAODV and the performance metrics for analyzing the network performance. The metrics considered for the evaluation of this scheme are:

i. Throughput,

ii. Goodput – Calculated for n nodes and is calculated as

$$G = \frac{\sum_{i=1}^{n} Packets_{Received}}{\sum_{i=1}^{n} Packets_{Originated}}$$

iii. Dropped Packets.

One metric is the resulting total Goodput *G* of a network with *n* nodes, i.e., the data forwarded to the correct destination for each node i. Goodput can be affected due to the intentional packet dropping from an intermediate node.

Overhead – As an overhead transmission cost are considered as most important for the energy consumption instead of internal computation.

$$Overhead(o) = \frac{TotalAlarm_{tx}}{TotalRREQ_{tx} + TotalRREP_{tx} + Error_{tx}}$$

The transmission overhead for various packets from MAODV and CONFIDANT protocol are:

MAODV control messages -

- Route Request (RREQ)
- Route Reply (RREP)
- Multicast Route Activation (MACT)
- Group-Hello (GRPH)
- Neighbor-Hello

Confidant control messages - ALARM Messages transmitted as an extension of routing protocol that is used as warning messages.

5. CONCLUSION

In this paper, we propose to implement a multicast protocol M-CONFIDANT, a security enhancement algorithm to detect selfish nodes. To encourage packet forwarding among nodes and discipline the selfish behavior in non- cooperative ad hoc network environment. This node behavior is monitored during route discovery thus effective identification of selfish nodes. The network performance is to measured that remains a concern for multicast overhead incurred for communication.

6. ACKNOWLEDGMENTS

I wish to express my deep gratitude to Dr. M. K. Rai**,** Associate Professor and Mr. Nitin Umesh, Assistant Professor, Lovely Professional University for providing their uncanny guidance, motivation and support throughout the preparation of the report.

7. REFERENCES

[1] S. Buchegger and J.-Y. Le Boudec 2002. Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). In J. Hubaux, J. J. Garcia Luna-Aceves, and D. Johnson, editors, Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, Switzerland, June 9-11, 2002, pages 226–236. ACM Press, June 2002.

[2] Shane Balfe, Po-Wah Yau and Kenneth G. Paterson. A Guide to Trust in Mobile Ad Hoc Networks

[3] Malamati Louta, Stylianos Kraounakis and Angelos Michalas. A survey on reputation-based cooperation enforcement schemes in wireless ad hoc networks.

[4] Jos´e Montero-Castillo and Esther Palomar 2011. Cooperation in Ad Hoc Network Security Services:Classification and Survey. In UBICOMM 2011: The Fifth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2011.

[5] Royer, E. M. and Perkins, C. E., 2000. Multicast Ad hoc On-Demand Distance Vector (MAODV) Routing. In IETF, Intemet Draft: draft- ietf-manet-maodv-00.txt, 2000.

[6] Yufang Zhu and Thomas Kunz 2004. MAODV Implementation for NS-2.26. In Systems and Computing Engineering, Carleton University, Technical Report SCE-04-01, January 2004.

[7] Abeer Ghandar, Eman Shabaan and Zaky Fayed, 2011. Performance Analysis of Observation Based Cooperation Enforcement in Ad Hoc Networks. In IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011.

[8] Pietro Michiardi, Refik Molva, CORE: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, IFIP CMS02, Communication and Multimedia Security Conference, September 2002

[9] Priyanka Goyal, Vinti Parmar and Rahul Rishi, 2011. MANET: Vulnerabilities, Challenges, Attacks, Application. In IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[10] Renu Dalal, Manju Khari and Yudhvir Singh, 2012. Different Ways to Achieve Trust in MANET. In International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.

[11] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, 2012. The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad–hoc Networks. In International Journal of Recent Technology and Engineering (IJRTE), Volume-2, Issue-2, December 2012.

[12] Qi He, Dapeng Wu and Pradeep Khosla, 2004. SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks.