ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (177-187), Month: July - September 2016, Available at: www.researchpublish.com

Truthful Detection of Packet Dropping Attacks in Opportunistic Mobile Networks

Aswathy Mohan[1], Sankari S[2]

[1]M.G University, [2]Anna University
[1]Mount Zion College of Engineering, Pathanamthitta, India, [2]S.Verrasami Chettiar College of Engineering and Technology,Thirunelveli,India

Abstract: **Cooperation among nodes is the fundamental requirement for the Opportunistic Mobile Networks (OMNs).Here using the store-carry-and-forward mechanism, messages are processing the communication. Each and every node in the network has a mobility and range of region in which each node communicate with other node or its neighbour node. Due to the dynamic nature, several security threats arise in such networks. The selfish behaviour of nodes affects the overall performance of the packet transmission. In OMNs, truthfully detected the packet dropping on the basis of holding procedure schemes. When sensor data is transmitted towards the sink along the tree structure, each packet sender or forwarder adds a small number of additional bits, to the packet, which is called packet marks. Packet marks is each time modified by the corresponding node. Using Packet marks the sink can figure out the dropping rate associated with every sensor node. Packet mark based on CR Score, it indicates how much we can trust the node and measures the degree of selfishness. After detecting the selfish node and create SCF tree and allocate the replica to overcome the selfish nodes. Identifying the packet dropper and runs node categorization algorithm and heuristic ranking algorithm for providing the knowledge that which nodes are bad for sure and which nodes are suspiciously bad. Proposed method identifying the multiple selfish node attacks and overcome these selfish nodes using replica allocation and credit risk score techniques.**

Keywords: **Cooperation, Opportunistic Mobile Network, Credit Risk Score, Self Centered Friendship Tree.**

I. INTRODUCTION

Opportunistic Mobile Networks (OMNs) are a category of delay-tolerant-networks (DTNs). Delay Tolerant Networking (DTN) is a communication networking pattern that provides a communication environments where there may be no end-to-end paths, or continuous path, communication opportunities change and their interval can be very lengthy and not even identified beforehand. Routing messages in this type of environments can be reasonably different compared to traditional networks. OMNs are routing their path opportunistically from source to destination using store-carry and forward mechanism. The mobility among nodes in the network which create new opportunity to communicate with one another. Here the path exists between source and destination pairs might not be connected at the same time. Each node which are typically computed the routes based on the local information of the node. When Source node and destination node are in contact, it delivers the message to destination node otherwise the message is forwarded to the intermediate node. The intermediate node which store and carry the message until one of them meets the destination node and forward to it or they can find other nodes.

The MDR based cooperation adaptation in wireless networking is considerably depends on cooperation of the intermediate nodes. . Each and every node in the network has a mobility and range of region in which each node communicate with other node or its neighbour node. For avoiding the confusion and complexity in topological interface, provide a parent node capacity to each node in the network based on user requirement. Cooperation strategy is based on Message Delivery Ratio (MDR). The system mainly use three cooperation adaptation criteria, which are cooperator, exploiters, isolators are based on Distributed Information Based Cooperation Ushering Scheme (DISCUSS). The nodes

which preserve the exchange information with one another during contacts about the message created and delivered in the network. Based on this information nodes are evaluate their own performance and evaluate with network performance and adapt most successful forwarding strategy. The evaluation is based on message delivery ratio. If the nodes are not in contact, receive the appropriate information from global knowledge and precede the communication and enhance the reliability and lossless communication. The present routing protocol which provide a hypothesis that nodes are fully cooperative. The every node in the network has their own goals, so we not considered a fully cooperation. Since typically it is unmanaged. Some nodes which shown a selfish behaviour. Some nodes may take help from others for forwarding their message but may not always assist in forward others message. It will affect the overall network performance. The selfish behaviour detection is one of the important criteria. These selfish nodes are sometimes shows the dropping behaviour .The dropping occurs when the message or data on holding. Based on that holding procedure, identify the CR score and develop the SCF tree.

II. EXISTING SYSTEM

OMN is generally reliant upon cooperation by intermediate nodes. Existing system which uses different cooperation enforcing schema and security enhancing schemes. The cooperation enforcing techniques are mainly based on credit based schema and reputation based schema. In credit based schema virtual currency or pricing acts as the credit. Different types of credit based schema used in existing systems. In reputation based schema, Reputation of the nodes is calculated by their neighbours based on the message forwarding actions. It Need a offline system manager. when each node register to join the network .Reputation value is assigned to the forwarding node. Nodes are not accepted when their corresponding reputation are less than a given threshold.

MDR Based Cooperative Strategy Adaptation in Wireless Networks [1], which enhance the cooperation among nodes and improves the network performance. To improve security, proposed a credit based schemes, virtual currency or pricing act as a credit. MOBICENT: a Credit based incentive system [2] to motivate the selfish nodes to cooperation. It provides incentive to the selfish nodes for forwarding other node's messages. Another one credit based schemes, A Practical Incentive protocol (PI) for DTNs [3] where the selfish nodes are stimulated to cooperate by forwarding the message of other nodes. Pi attaches incentives to the messages and sends it to the intermediate nodes, which attracts the participation of other nodes in forwarding. SMART, a Secure Multilayer Credit based incentive Scheme for DTNs [4]. SMART stimulates cooperation among nodes by preventing the malicious users from fraud credits based on layered coins. Layered coin provides implicit credits for charging and satisfying of data forwarding in DTNs. However, this method needs a trusted authority for storing the credit and reputation of each node.

Reputation based scheme is a reputation-based incentive scheme. Reputations of the nodes are calculated by their neighbours based on the message forwarding actions. Need an offline system manager. When each node registered to join the network, Reputation value is assigned to the forwarding node. Nodes are ostracized when their corresponding reputation are less than a given threshold. Proposed a practical reputation based incentive "PRI" scheme [5]. PRI also assumes the use of offline security manager (OSM), which is indicting of key distribution. Nodes register in OSM before joining the network. It a require a tamper proof hardware for updating the reputation values of every node. Giving reward and punishment, the recipient nodes need to be traced and need a central authority. Identification of malicious packet loss during routing misbehaviour [6], address a scheme to mitigate routing misbehaviour by off putting the number of packets forwarded to the misbehaving nodes. It keep the signed contact record of its previous contacts and identify the node has dropped any packet. Detection and Isolation of selective packet drop attack [7]. There is much vulnerability in selective packet drop attack which can be avoided or removed with help of monitor nodes. In Cognitive radio adhoc networks ,Detecting multiple selfish attack nodes using replica allocation [8], which detect the selfish behaviour and provide proper replica allocation in Cognitive radio networks. For avoiding these vulnerabilities by introducing a truthful detection and prevention of packet dropping attack in opportunistic mobile networks.

III. SYSTEM MODEL

In OMNs, there is no any infrastructure and it shows dynamic topology. All nodes are projected to take part in the forwarding process in order to increase the communication opportunities. This creates the problem of selfish behaviour.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (177-187), Month: July - September 2016, Available at: www.researchpublish.com

Nodes are tending to forward only packets that concern them while ignoring others. This problem is even further dangerous for small devices as shortage of resources fosters selfish behaviour. Nodes need incentives with the purpose of cooperate with each other for excellent communications. Currency based cooperation enforcement schemes rely either on expensive tamperproof hardware or on an online trusted third party which is not compatible with the delay tolerance characteristic. Reputation mechanisms require stable network configuration and a large amount of time to establish trust. Proposal fully concentrated on the main security issues in OMN, such as selfish attack and packet dropping behaviour. Giving reward and punishment, the recipient nodes need to be traced and It Need a central authority, which is costlier in OMNs.

In opportunistic mobile network the main problem is unreliable communication and loss communication. To enhance the reliable communication will ensure the cooperation among the nodes. For enhance the cooperation of each node to analyze the strategy of each node and increase the message delivery ratio. Proposed system, promote cooperation based on DISCUSS and its variant on DISCUSS with global knowledge. In DISCUSS scheme, the nodes reliably exchange information with their neighbour nodes. In DISCUSS with global knowledge, the nodes can obtain message delivery information from a central knowledge. Each node follows any one of these message strategy.

1. *Cooperate:* - Forward their own message and other's message

2. *Exploit:* - Forward their own message and drop other's message

3. *Isolate:*-Only receive the message which they are destination. They don't take help from other and don't do

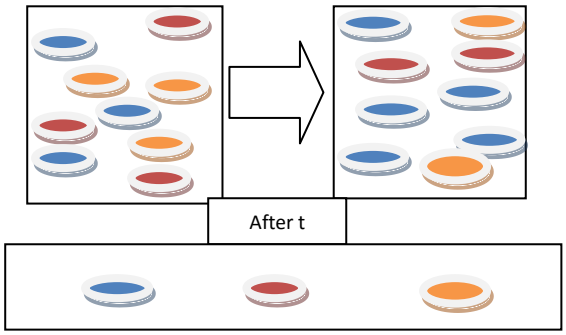


Fig 1: Strategy adaptation of nodes after a t time

The DISCUSS system architecture consist of three phases, they are node generation, cluster formation, packet forwarding.

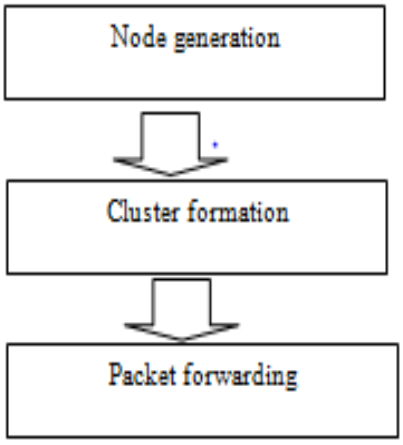


Fig 2: Proposed system architecture

a. Node generation

Node generation is the initial phase in which the network of nodes are formed. In this phase , should specify the node id, node type, node position, number of nodes, node link etc. based on that elements source and destination nodes also specifies and processing node integration and results are forward to the input of cluster formation phase.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (177-187), Month: July - September 2016, Available at: www.researchpublish.com

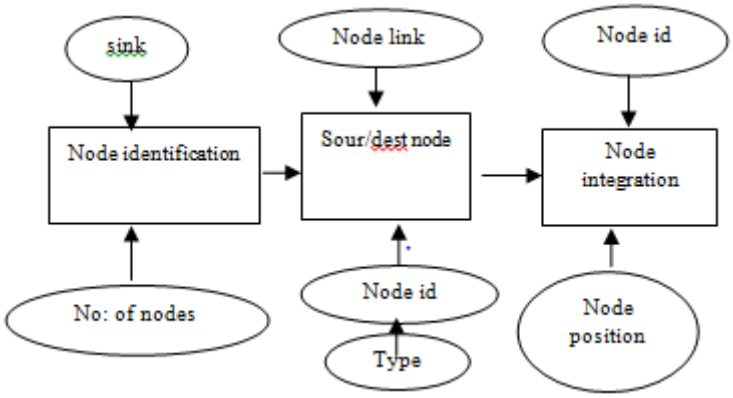


Fig 3: Node generation

b. Cluster formation

Cluster formation is the second phase in which form the different clusters based on number of nodes and calculate energy level and cluster head. The energy level calculations are based on the battery level of nodes and finally construct the route table. That result of route table which promote to next phase

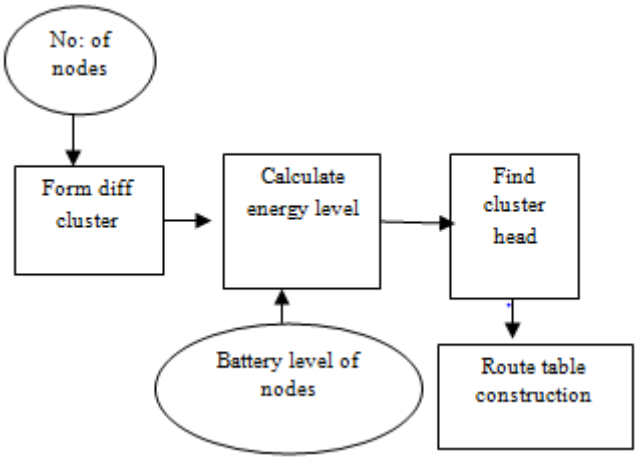


Fig 4: Cluster formation

c. Packet forwarding

Packet forwarding is the final phase , find out the available cluster head and proceeding the routing . on the basic of performing the routing, data are collected and transferred to base station and update the route table.

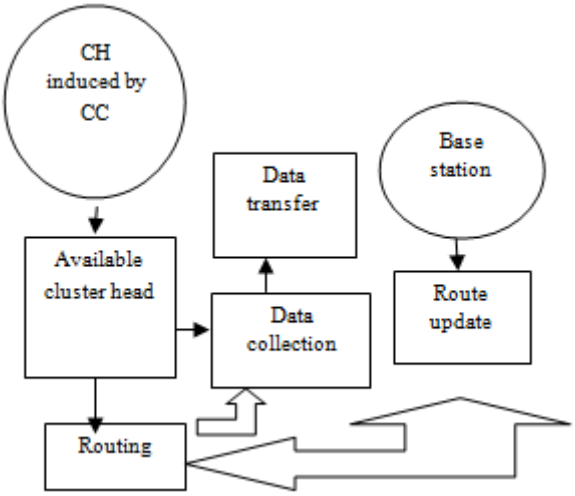


Fig 5: Packet forwarding

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (177-187), Month: July - September 2016, Available at: www.researchpublish.com

IV. PROPOSED SYSTEM

1. Proposed DISCUSS Design

The proposed system which enforcing the cooperation of nodes using DISCUSS techniques. The designing of the DISCUSS system comprised of four steps. They are topology creation, message transfer, opportunistic mobile network, distributed information.

Topology Creation

It has not a specific topology, because each topology will be changed due to the movement of the nodes at each t time. Sensor nodes form a DAG and take out a routing tree from DAG. When a node wants to send out a packet, it attaches a sequence number with it, encrypts the packets and then forward packet to parent on the routing tree. The routing tree is reshaped every round. As a certain number of rounds have passed, the sink will have collected information about node behaviours in different routing topologies. The purpose of system initialization is to set up the DAG and the routing tree to facilitate packet forwarding from every sensor node to the sink. Each sensor node u is preloaded the following information:

Np: The maximum number of parent nodes that each node records during the DAG establishment procedure.

Ns: The maximum packet sequence number. For every sensor node, its first packet has sequence number 1, the Ns^{th} packet is numbered Ns and so on and so forth.

Message Transfer

When an innocent intermediate node receives a packet, it attaches a random variable to mark the forwarding path of the packet, and then forwards the packet to its parent. A mischievous intermediate node may drop a packet it receives the intermediate node may either drop or modify the packets before sending to sink. On receiving a packet, the sink node decrypts it, and thus finds out the original sender and the packet sequence number. The sequence numbers of received packets for every node tracked by sink node and for every certain time interval, which we call a round. it calculates the packet dropping ratio for every node. Based on the dropping ratio and the facts of the topology, the sink node identifies packet droppers.

Opportunistic mobile network

Represent an OMN as (N; M; S), where N denotes the set of nodes in the network. M denotes the set of messages generated by the nodes. S denotes the set of strategies selected by any node in forwarding the messages (Cooperate; Exploit; Isolate). Each node may act as a source, a destination or an intermediate relay node**.** We consider three group of nodes cooperators, exploiters, and isolators based on these strategies. The following section elaborates the behaviour of the individual nodes.

1. *Cooperators*

These nodes with the strategy “cooperate” not only forward their own messages, but help the other nodes as well in doing so. In other words, the co operators act as relays by receiving, storing and forwarding the messages generated by the other nodes.

2. *Exploiters*

On the other hand, the exploiters forward their messages to the other nodes (co operators) for delivery. They receive other node’s messages, but instead of storing them, they silently drop those messages. The exploiters take help from others for forwarding their own messages as free riders, without helping them.

3. *Isolators*

The isolators only receive the message for which they are the destinations. They do not take help from the other nodes for forwarding their messages, neither do so for others. The isolators directly deliver their messages, when they meet with the corresponding destination node.

Distributed information

When a node dynamically switches its forwarding strategy, if required, to the most successful strategy in the concerned SD-OMN. Strategy defined OMN is a combination of N, M, S. N is denoted the set of nodes, M is denoted set of

messages, S is denoted set of strategy selected(C, E, I).i.e., Nc+Ne+Ni=|N|. The Node shares their relevant information. They are

- Received message ID
- Message sender node ID
- Own delivery probability

It comprises of two phases that are repeated in every generation interval (t).

(1) Acquiring information on the performance of the SD-OMN.

(2) Strategy adaptation

The first phase requires information on

(a) The messages created (CM) by the nodes

(b) The delivered messages (DM)

(c) The delivery probabilities (DP) of the nodes.

In this module Categorization and Ranking will be performed based on the node behaviour. If there is any modification or drop of packets in node it assumes negative value for modifier or dropper. The categorization of nodes can be taken in any one of the following cases.

- Packet droppers for sure.
- Suspicious packet droppers.
- No packet droppers for sure

2. Procedure of DISCUSS

The DISCUSS steps in the proposed system are as follows.

STEP 1: Start

STEP 2: Exchange information with nodes

STEP 3: Compute own delivery probability

STEP 4: Computed group wise weighted delivery probability(yc,ye,yi)

STEP 5: Compute P<max (yc,ye,yi), if it true then step 6 ELSE GO TO Step 8

STEP 6: Calculate G succ = arg max (yk), k∈yc,ye,yi

STEP 7: Set on strategy as G succ.

STEP 8: Stop

3. Proposed System's Strategy

Proposed system mainly based on DISCUSS and DISCUSS with global knowledge.

Discuss: In Discuss scheme the nodes are reliably exchange their information during the contact.

Discuss with global knowledge: For the sake of richness ,effectiveness and evaluating the success, we also think a version of DISCUSS, where the nodes have absolute information about the Strategy defined in OMN. In this case, imagine the occurrence of a central authority in the network, with which the nodes can communicate directly. Whenever a new message is created (or delivered), the central authority is informed by the disturbed node. Based on these information, the central authority calculate the delivery probability of each node. At the end of each t, all the nodes get the delivery probability knowledge of all the other nodes from the central authority. Based on this, most successful strategy adapted by the node, if required.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (177-187), Month: July - September 2016, Available at: www.researchpublish.com

4. Design of DISCUSS

With the help of UML tools the design is supported. It represents how the proposed system working. The data flow diagram based on the steps in DISCUSS depicted below:

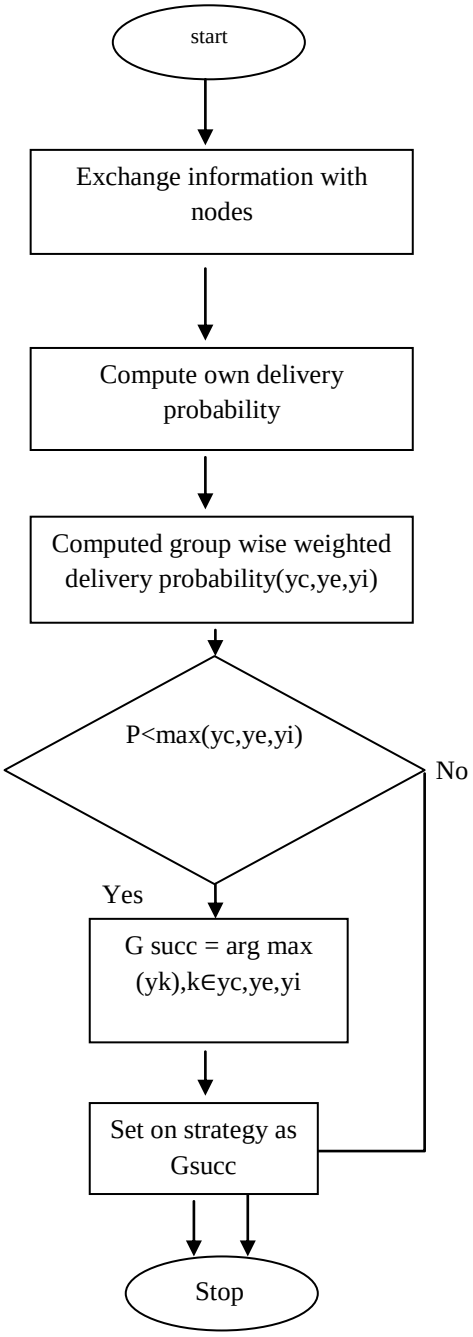


Fig 6: Flowchart depicting the steps in DISCUSS

5. Proposed detection of packet dropping attacks

The Proposed system not only gives importants to cooperation among nodes but also give priority to prevent attacks in OMNs. For the good security and Privacy issue, introduce a truthful detection of packet dropping attacks in OMNs. The proposed method is used to compute the multiple selfish nodes in opportunistic mobile network and to overcome those selfish nodes using replica allocation.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (177-187), Month: July - September 2016, Available at: www.researchpublish.com

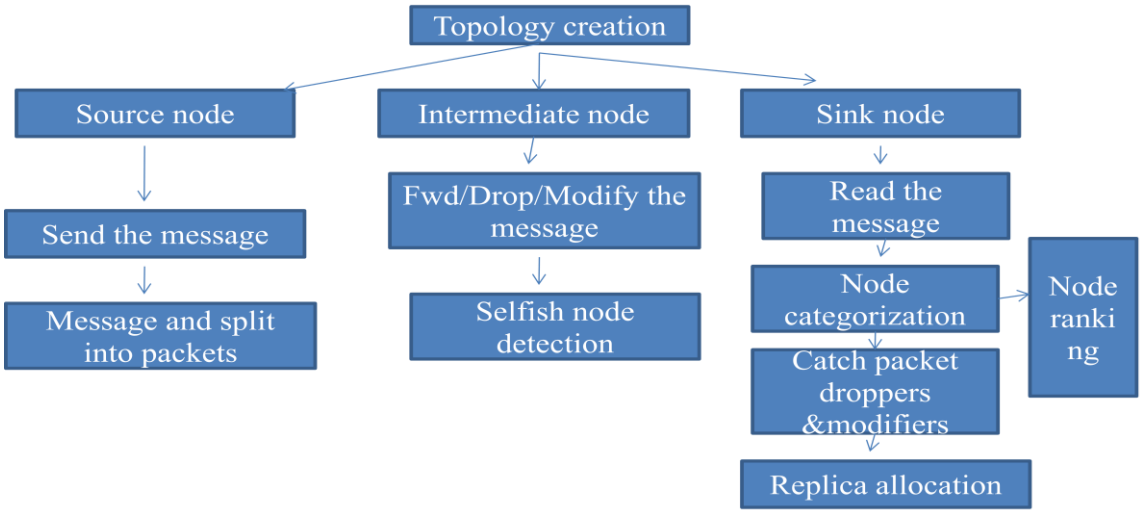


Fig 7: Architecture of detection of packet dropping attack

When sensor data is transmitted towards the sink along the tree structure, each packet sender or forwarder adds a small number of additional bits, to the packet, which is called packet marks. Packet marks is each time modified by the corresponding node. Using Packet marks the sink can figure out the dropping rate associated with every sensor node. Packet mark based on CR Score, it indicates how much we can trust the node and measures the degree of selfishness. After detecting the selfish node and create SCF tree and allocate the replica to overcome the selfish nodes. Identifying the packet dropper and runs node categorization algorithm and heuristic ranking algorithm for providing the knowledge that which nodes are bad for sure and which nodes are suspiciously bad. Proposed method identifying the multiple selfish node attacks and overcome these selfish nodes using replica allocation and credit risk score techniques.

6. Design of packet dropping attack detection

The truthful detection of packet dropping attacks design which consist of four modules. They are Selfish Node Detection, Building SCF Tree, Replica Allocation, Identification Of Packet Dropper .

a. Selfish node detection.

When a node Ni makes an admittance request to a data item (i.e., issuing a query), it checks its own memory space first. Ni holds the original or replica of the data item in its local memory when request is successful. The request will be broadcast if it does not hold the original data or replica. The request is also successful when Ni receives any reply from at least one node associated to Ni with one hop or multiple hops, which holds the original or replica of the targeted data item. Otherwise it leads to the failure of request or query processing. When a node Ni receives a data access request, it either

1) Process the request by sending its original or replica if it holds the target data item (the data may experience multiple hops before reaching the requester)

2) Forward the request to its neighbours if it does not hold the target data item.

The CR score is created or updated consequently during the query processing phase by the measure of degree of selfishness. In other words, CR score is based on the degree of selfishness. The measure of Credit Risk Score is how much we can trust that node. A node desires to know if another node is convincing or believable, in the sense that a replica can be paid back, or served upon request to share a memory space in a the networks.

Packet transmission from S node to D node which route is shortest among all possible routes. If any node acts like selfish node in OMNs, then that node is not ready to transmit packets to other node. It affects the communication very badly. So in network the selfish node detection is essential for efficient communication by applying “degree of selfishness” formula for each node. . Each node should calculate the credit risk score of each node which is connected to it. Estimate the degree of selfishness of all its connected node based on the CR score.

Credit Score=Expected risk/Expected Value

To estimate the degree of selfishness, first illustrate the characteristics of the selfish node that may lead the selfish replica allocation difficulty and determine both expected risk and expected value.

b. Building SCF Tree

The SCF tree based replica allocation techniques are motivated by human friendship management in the real world, where each person makes his/her own friends creating a web and manages friendship by himself/herself. He/she does not have to examine these with others to preserve the friendship. The main purpose of our novel replica allocation techniques is to diminish traffic overhead, to achieve the high data accessibility. If the novel replica allocation techniques can assign replica without discussion with other nodes then the traffic transparency or overhead will decrease. The main aim of the SCF tree based replica allocation techniques is that it can decrease the communication cost, while achieving high data accessibility. This is because each node identifies selfishness and makes replica allocation at its own judgment, without forming any group or engaging in lengthy negotiations.

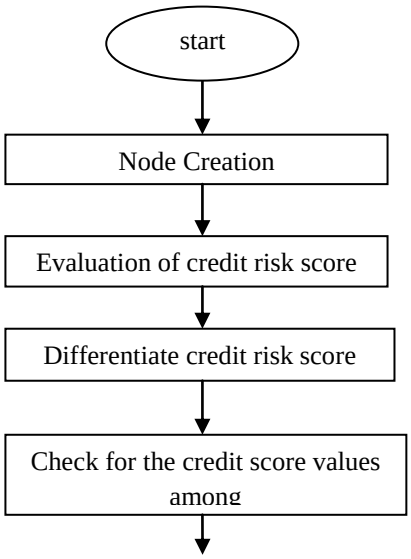
c. Replica allocation

A node allocates replica at each relocation period after building the SCF tree. Each node asks non selfish nodes within its SCF tree to embrace replica when it cannot hold replica in its local memory space. In a fully distributed manner the SCF tree based replica allocation is performed, each node determines replica allocation independently without any communication with other nodes. Since every node has its own SCF tree, it can perform replica allocation at its judgment.

For example, after building the SCF tree, N1 may ask N2 to hold some replicas. Note that the decision, whether to accept the replica allocation request or not, will be made at N2's discretion (if N2 is selfish, it may not accept the replica allocation request). Afterward, node N1 may issue a query for the replicas. At this time, N1 is likely to identify whether the expected N2 serves the query (i.e., non selfish) or not (i.e., selfish). Since we imagine that a node can use some segment of its memory space selfishly, we may divide memory space Mi for replica logically into two parts: selfish area Ms and public area Mp. Each node may use its own memory space Mi freely as Ms and/or Mp. In each node, Ms will be used for data of local interest.

d. Identification of packet dropper

Identifying packet droppers and modifiers, the system initialization phase is followed by several equal duration rounds of burglar detection phases. The sensor nodes form a dynamic routing tree at the sink in the initialization phase. The data traffic is transmitted through the routing tree to the sink in each round and each packet sender/forwarder adds a small number of additional bits to the packet and also encrypts the packet. When one round finishes, based on the additional bits carried in the received packets, the sink runs the node categorization algorithm to identify nodes that must be droppers or modifiers and nodes that are suspiciously bad. The sink will have collected information about node behaviours in different routing topologies as a certain number of rounds have passed. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and topological relationship of nodes. The heuristic ranking algorithms run by the sink for further identify bad nodes from the large number of suspiciously bad nodes.



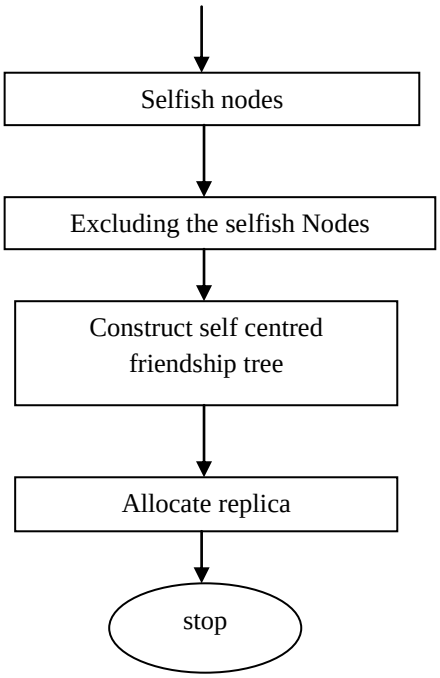


Fig 8: Flowchart for detecting the steps in selfish nodes.

V. CONCLUSION

In this work, The proposed a distributed cooperation mechanism, named DISCUSS, for converting the non cooperate nodes to cooperate. After a generation interval each node compares its performance with performance of other groups and adapt a most successful strategy .we have identified the multiple selfish node attacks and overcome these selfish nodes using replica allocation technique. The proposed method detects multiple selfish nodes attack using credit risk score. This detection method is very reliable. In DISCUSS, the strategy is based on message delivery ratio. It enhances the reliable communication and lossless communication. Improve the network performance and reduce the traffic overhead and communication cost. For the sake of totality and evaluating the effectiveness, we also consider a version of DISCUSS, where all nodes have absolute information about the Strategy defined OMN. In this case, we consider the inclusion of a central authority in the network, with which the nodes can communicate immediately. Whenever a new message is created (or delivered), the central authority is informed by the disturbed node. Based on these information, the central authority calculate the delivery probability of each node. At the end of each t, all the nodes get the delivery probability knowledge of all the other nodes from the central authority. Based on this, the nodes adapt their strategies to the most successful one, if required.

ACKNOWLEDGEMENT

I would like to extend my thankfulness to the reference authors, as well as reviewer of my paper.

REFERENCES

[1] Aswathy Mohan, Smita C Thomas "MDR Based Cooperative Strategy Adaptation in Wireless Communication," in ., IJEER Vol. 4, Issue 1, pp: (64-71), Month: January - March 2016

[2] B. B. Chen and M. C. Chan, "MobiCent: A credit-based incentive system for disruption tolerant network," in Proc. IEEE Conf. Com- put. Commun., 2010, pp. 875–883.

[3] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," IEEE Trans. Wireless Commun., vol. 9, no. 4, pp. 1483–1493, Apr. 2010.

[4] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Yanfei Fan, and Xuemin Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Transactions On Vehicular Technology, Vol. 58, No. 8, October 2009

[5] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," ACM SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, pp. 19–20, 2003.

[6] K.P. Kaliyamurthie, D. Parameswari and R. Udayakumar, "Malicious Packet Loss During Routing Misbehavior-Identification," Middle-East Journal of Scientific Research 20 (11): 1413-1416, 2014.

[7] Er. Priyanka Goel , Dr. Pankaj Kumar Verma, "Detection And Isolation Of Selective Packet Drop Attack In Manet Using Diffie - Hellman Algorithm," International Journal of Latest Research in Science and Technology Volume 3, Issue 3: Page No. 137-139, May-June 2014.

[8] Kiruthiga S, Leeban Moses M , "Detecting Multiple Selfish Attack Nodes Using Replica Allocation in Cognitive Radio Ad-Hoc Networks" IEEE Trans. Wireless Commun., IJIET vol. 5, issue 2 April 2015.