Social-aware Context Based Approach for Forwarding Data in Wireless Network Comprising of Selfish Individuals

Bency Wilson
Department of Information Technology
Rajagiri School of Engineering & Technology, Rajagiri Valley P O
Kochi-39,India
bencywilson@gmail.com

Preetha K G
Department of Information Technology
Rajagiri School of Engineering & Technology, Rajagiri Valley P O
Kochi-39,India
preetha_kg@rajagiritech.ac.in

Abstract—In social based mobility network comprises of selfish individuals that are not willing to forward the packets but wants to forward their own messages. Proposed system uses a context based protocol that can be used in social aware network like PSN. Here suggests a method to effectively detect selfish nodes from the network. It helps to differentiate selfish nodes from broken and overloaded nodes. In adhoc network throughput increases when all available nodes are used for routing and forwarding. So instead of avoiding selfish nodes from the routing path as mentioned in existing solutions can effectively utilizes all the existing nodes The proposed system also suggests a method to avoid selfish behavior among the nodes and a method to make the selfish nodes forward the message without any hesitation. For transferring the data using selfish nodes uses an enhanced epidemic forwarding protocol in the system.

Keywords- PSN; selfish; epidemic; routing; context**.**

I. INTRODUCTION

Internet users can access all the network applications if there exists internet connectivity within the device. When a user needs to transmit data to other needs a reliable connection between the users .That means the other user needs to be in the wireless range or has corresponding wireless capabilities. In effect all users need end-to end connectivity for reliable data transfer. If there exists no continuous connectivity between the users the data delivery rate will decrease considerably. In reality the networking architecture is unstable and the data is transferred within a stressed environment. The network is subjected to frequent and long lasting disconnection which interrupts the data transfer and increases the error rate. So here deals with a network that is based on sociality called Pocket Switched Networking (PSN) [5].

PSN aims at providing network services without in need of an end to end connectivity or internet connectivity islands. In PSN the carriers are human beings. Data is forwarded among the handheld devices with human beings using local/global connectivity. Such devices include mobile Phones, PDA, laptops etc. Since broken time is more, PSN offers better packet delivery by using store and forward approach. PSN also reduces the cost and delay in forwarding the data outside the connectivity islands. PSN doesn't rely on any particular infrastructure so they are used in rural and developing regions for providing low cost communications when infrastructures fail due to natural disasters or other failures.

The main challenge exists in PSN are caused due to Mobility, Sociality, Selfish nodes, Security, Constraints on energy and storage. Mobility induces challenging to communicate with users, as forwarding paths may be unstable and reachability of device may be highly variable. In the real world scenario, human beings are selfish in nature. As a result, people may not be willing to forward others data. So a selfish node may not forward data for anybody. The selfish node misbehaves by acting as message droppers and not willing to spend their own resources such as energy, memory for others. This kind of routing misbehaviour reduces the packet delivery ratio.

The main scenarios of PSN include search-and-rescue, military and law enforcement operations. In these all users are working to achieve a common goal. So it's obvious that if some of the nodes deviate selfishly, after a while everybody will. This will interrupt the routing and packet forwarding between the nodes. Methods to mitigate routing misbehavior in MANET cannot be applied to PSN due to its frequent disconnected links. There exists an incentive mechanism that encourages the node to forward other people messages. Another scheme is to preventing or punishing those from sending their own messages.

The paper deals with various methods adopted to avoid the problem caused by the selfish nodes in forwarding the packets and in the approach G2G epidemic forwarding uses some forwarding mechanisms to forward the message to respective nodes [1].

The rest of this paper is organized as follows. Section 2 provides an idea on the existing solutions. Section 3 elaborates the related works. Proposed System is explained in section 4.Conclusion is in section 5.

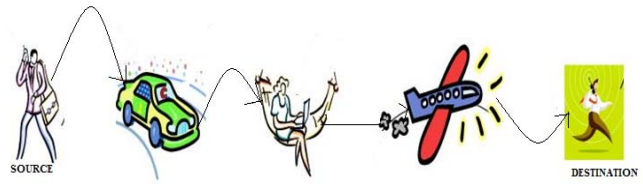

Figure 1: Pocket switched network

II. EXISTING SOLUTIONS

A lot of research is going on in the area of building efficient forwarding protocols for PSN. The existing solutions for data forwarding among selfish individuals include reputation-based schemes, credit based schemes and context based schemes.

A. Reputation Based Scheme

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Here nodes will collectively detect the misbehaving nodes in the network and propagate that information about the selfish nodes throughout the entire network. Here each node makes reputation about other nodes in the network. If a node acts as message dropper, then it will get bad reputation. The main drawback of this approach is that the selfish nodes are isolated from the system. In social network all the nodes eventually exhibit the behavior of selfishness. So there is a possibility that all nodes are isolated which in turn affects the packet delivery ratio and increases error rate of the network. Another challenge deals with the propagation of the reputation information in secured ways and it can't resist collusions also. The reputation based schemes are not capable of detecting the message droppers accurately, since due to collision also packets can be dropped. So the network condition effects the detection of selfish nodes.

B. Credit Based Schemes

In credit based schemes each node get paid for the service they are providing Here each node gets credits for forwarding data to others in the form of credits or virtual money. To forward its own data, the node can make use of those collected credits to forward its own data. In the case of selfish nodes they don't have credits to send their data. So this scheme will compel each node to propagate messages. The main drawback of this approach is that it needs complex systems called virtual banks to manage the credits of each node and needs separate hardware modules to impose security. Also a node can misbehave by dropping the messages after collecting enough credits.

C. Context Based Schemes

In context based schemes, a node is evaluated in terms of its reputation or credit and its context is recorded. The limitation of this approach is that it requires continuous uninterrupted tracking of each node to collect details about its behaviour of forwarding all packets in multiple paths. Finally the selfish node is punished by avoiding them. That result in longer routing path after bypassing the selfish nodes. Here we measure the nodes behaviour in packet transmission. This may cause complexity and can affect accuracy. Also the measurement results of each node have to be exchanged among themselves, which creates the problem of ensuring trust among nodes. Security of storing, updating and exchanging context data is another problem in context based scheme.

III. RELATED WORK

In [4] Marti et al. proposed a scheme that comes under reputation based scheme. *Watchdog* to identify selfish behaviour of each node, and used *Path rater* to choose a reliable path for forwarding. Here when a node transmits data its neighbour will promiscuously listens to that transmission to verify whether it's forwarding the data or not. If the corresponding node drops packet, then it's misbehaving. Pathrater uses this knowledge to choose a reliable network path. Watchdog done this by maintaining recently send packets in its memory and compares overheard packet with each in memory. If matches, packet is removed from memory else if packet

remains more than a timeout; watch node will increment a failure tally for that node. If tally is greater than threshold then neighbour node is misbehaving and notifies the source. Drawback of this approach is that watchdog went wrong when there exists a collision.

Buchegger proposed *CONFIDENT* protocol in [3], which uses reputation scheme to detect selfish nodes and to isolate them. Here it uses a path manager whose function is to delete the selfish nodes from the path, According to the reputation of each node in the path, performs path re-ranking etc. If the path manager detects selfish node to convey warning information, an ALARM message is sent by it containing the address of observed node. Its shortcoming is that after isolating the selfish nodes from the network, only less no: of nodes can participate in routing and forwarding. This will reduce network throughput, bandwidth and results in network partition.

In [7], Buttyan proposed a payment scheme which is a credit scheme called *Nuglets* .In that work, the payment units are called *Nuglets* and uses a separate hardware module on each node. This scheme helps to reduce congestion in the network and nodes are not interested in sending unwanted messages and overload the network because this would decrease its number of nuggets and to earn nuggets each node will be willing to forward others messages too. The paper explains two approaches: the Packet Purse Model and the Packet Trade Model to. But this scheme requires separate hardware modules to manage the credits of each node and after getting enough Nuglets a node can misbehave.

In [1] uses two protocols for forwarding packet in a social mobile network with nodes having selfish behaviour: Give2Get (G2G) Epidemic Forwarding and Give2Get Delegation Forwarding. In G2G Epidemic Forwarding each node will relay the message to first two nodes it meets. This will consume available bandwidth and affects the network throughput. Here each node should collect POR [proof of relay] after forwarding to the immediate neighbours to show to CA that it's not misbehaving. Collecting POR also incurs additional cost and affects Packet delivery ratio. In G2G Delegation Forwarding each message is forwarded only after checking the forwarding quality of the next relay node. This will reduce the cost of forwarding and no: of replicas.

IV. PROPOSAL FOR IMPROVEMENT

The proposed system suggests method to detect the selfish nodes in the network and proposes a mechanism to make selfish node to forward the messages by reducing available bandwidth and propagation delay. It's a social aware context based approach named as SAC. It makes use of DSR (Dynamic source routing) protocol for data forwarding.

A. To Detect a Selfish Node Precisely

In this system model, every node is selfish. Introduce a central authority (CA) to handle joining of new nodes in the network. In a social aware network detection of selfish nodes are crucial. Selfishness is mainly exhibited by dropping the messages. But the dropping can also be caused due to several other reasons like

a) Overloaded nodes: contains insufficient CPU cycles, bandwidth and other system resources.
b) Broken nodes: nodes containing faulty software etc.

To avoid this problem of accurate detection of selfish node SAC proposes a method to identify broken and overloaded node. To detect a broken node, each node should promiscuously monitor other nodes in its range. If the other node is in sleep state (i.e., not forwarding any of its packets) after a particular time frame, neighbours can intimate that information to others in its range by sending a short message without obstructing the packet transfer as in figure 2.

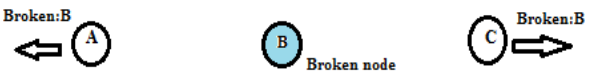

Figure 2: Broken Node

If a node is overloaded, that means it lacks enough resources for data transfer. Then it can intimate its neighbours by sending a short message to indicate it's overloaded. Then neighbours can choose an alternate path or can avoid the respective node from classifying it as selfish. If a node utilize this mechanism selfishly and continuously sends overloaded message then the neighbours can notify CA about its misbehaviour as shown in figure 3.

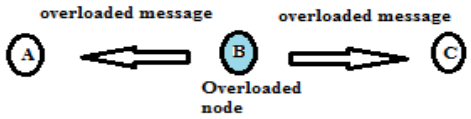

Figure 3: Overloaded Node

Using these methods can detect correctly a node is selfish or not. In existing techniques the selfish node is punished or avoided from data forwarding. If more nodes participate in routing data, then bandwidth increases, routing paths will become shorter, less chance for network partition. So need some techniques that make selfish nodes to forward data.

B. To Avoid Selfish Behavior Among Nodes

Each node should be unaware about the destination. Then only it will forward the data. For that the ID of the destination should be hidden to intermediate nodes within the routing path. For example in Figure 4, if A sends a message to B for D. When B checks the packet, destination is D. So B which is selfish will drop the message. To avoid this problem source can redefine the original path by including the id of destination more than once in the packet header. The packet header contains the Id of all nodes in the selected routing path. Since SAC protocol makes use of context information, it can choose previously available shortest paths for forwarding. For Example A defines the path as [A, B, C, D, N, D] in packet header instead of [A, B, C, D] and uses a layered encryption to provide security to payload and to hide the original destination. That means source node A encrypts the data using public key of nodes in the header in the reversed order i.e., pubB [pubC [pubD [pubN [pubD (data)]]]].

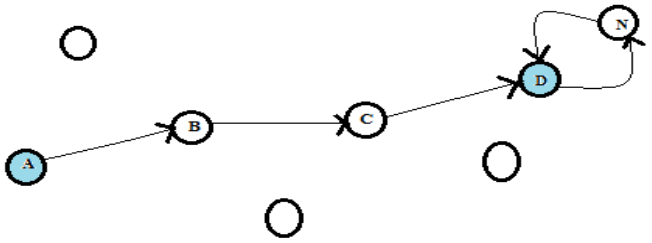

Figure 4: Redefined path

Each node can decrypt the data using their private key. If any nodes drops the message again, can use watchdog technique mentioned in [4] and can notify to CA. CA can verify the behaviour of the node by analysing the possibility of collision in the neighborhood of that node. When each node detects a selfish node can send a bad reputation message after signing the message using digital signature. This way can avoid the security problem in reputation scheme.CA can classify it as selfish. In this way can prevent collusion also.

CA can use G2G epidemic forwarding scheme mentioned in [1] to forward the packet. If a node is selfish CA sends a warning message to it. Then the selfish node must collect a POR [proof of relay] from its immediate neighbour after forwarding the message with a POR request to it. POR is used by the selfish node as a proof for CA. This scheme over utilizes the resources of each node. So every node will forward other's message without any hesitation.

V. CONCLUSION

The solutions for effectively forward data in social aware networks are facing a lot of challenges in networks such as PSN. By participating all available nodes in routing and forwarding can increase available bandwidth, throughput, creates shorter possible routing path and provides less possibility of network partition. Proposed system uses a context based social aware protocol that can be used in networks like PSN. Here suggests a method to effectively detect selfish nodes from the network containing broken and overloaded nodes. It also make use of all available nodes which helps to increase network throughput, bandwidth etc.

To avoid selfish behavior among the nodes a layered encryption and uses the concept of central authority(CA).It also covers a method to make the selfish nodes forward the message without any hesitation using an enhanced epidemic forwarding protocol.

REFERENCES

[1] Alessandro Mei, Julinda Stefa,"Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012.

[2] C. Song and Q. Zhang, "Coffee: A Context-free Protocol for Stimulating Data Forwarding in Wireless Ad Hoc Networks,"Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), 2009.

[3] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*,2002

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, 2000.

[5] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot,"Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM Workshop Delay-Tolerant Networking (WDTN '05), 2005.

[6] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott,"Impact of Human Mobility on the Design of Opportunistic

[7] L. Buttya´n and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc Wans," Proc. ACM MobiHoc '00, 2000.

[8] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," Technical Report CS-200006, DukeUniv., 2000.

[9] E.M. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant Manets," Proc. ACM MobiHoc '07,2007.

[10] A. Mei, G. Morabito, P. Santi, and J. Stefa, "Social-aware Stateless Forwarding in Pocket Switched Networks," Proc. IEEE INFOCOM '11, 2011.

[11] G. Resta and P. Santi, "The Effects of Node Cooperation Level on Routing Performance in Delay Tolerant Networks" Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), 2009.

[12] T. Spyropoulos, K. Psounis, and C.S. Raghavendra, "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks," Proc. ACM SIGCOMM Workshops, Aug. 2005.

[13] M. Grossglauser and D. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Networks," IEEE/ACM Trans. Networking, vol. 10, no. 4, pp. 477-486, Aug. 2002.

[14] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.