EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Integrated social network reputation inspired routing for effective data forwarding

Femilda Josephin Joseph Shobana[1*] and Ramaraj Narayanasamy[2]

Abstract

Wireless sensor networks face many threats which drain the energy. The performance of sensor network routing is much affected in the presence of selfish nodes with messages being delivered with a longer delay. Social network routing is a method in which the messages are selectively forwarded through the nodes where the encounters between these nodes are more likely to occur. Network reputations clearly speak about the quality of nodes involved in data forwarding. The idea is to utilise social network reputations of source or destinations for effective data forwarding in farmland sensor networks.

Keywords: Social networks; Epidemic routing; Wireless sensor network; Farmland sensor network; Collaborative; Opportunistic routing

1 Introduction

In wireless sensor networks (WSNs), nodes do not physically move in many directions. Instead, the nodes are at least temporarily static and are attached to a physical location until the task is done [1]. In case of any malfunctioning only, the sensor nodes disintegrate themselves from the network for a while until the problem is attended. After it is done, the sensor nodes generally reappear again bounded to the same previous physical location. If any such topological changes do exist, it shall be attempted by configuring themselves into the network [1].

However, the configuration of a new node involves registration in all necessary locations which would be time-consuming. The only solution is to insert the node at a desirable location and then allowing the node to communicate with the network on its own! This communication has to happen casually within fraction of seconds after the new node joins the network. The same is applicable when the old node rejoins the network. These requirements seemed to have been inspired from social network behaviour where there are no constraints or limitations in general on their collaborative or social behaviour except for security constraints. This social behaviour of WSNs shall be modelled via opportunistic networks.

In WSNs, the presence of selfish nodes may interrupt their cooperative behaviour and therefore trust and reputation mechanisms are widely practised in network routing. However, WSNs are a kind of delay-tolerant networks [2-4], in which nodes are enabled to communicate with each other even if a route connecting them never exists. These shall be modelled over opportunistic networks where the seed node grows into a larger network by extending invitations to join other nodes or node clusters or networks that it is able to contact. A new node that becomes a member of oppnet also called as helper can invite external nodes. All helpers collaborate on realizing the goals of the network.

In Figure 1, ‘S’ is the source node and ‘D’ is the destination node. At time ‘t1’, S and D are not in the same communication range, and hence, there is no connection between the source and destination node. Hence, the source node opportunistically uses the node ‘3’ to forward the data to destination. At time ‘t2’, node 3 forwards the data it holds to node ‘4’. At time ‘t3’, the nodes 4 and D are in the same communication range and hence the node 4 forwards the data to destination.

But the main problem which could be seen in this type of routing is that the nodes in the friends list might become malicious or selfish in the future. Hence, it is necessary to monitor the nodes in the friends list for finding the misbehaving nodes.

* Correspondence: femilda1@gmail.com
[1]Department of Computer Science and Engineering, Sri Lakshmi Ammal Engineering College, Thiruvanchery, Tambaram East, Chennai 600126, India
Full list of author information is available at the end of the article

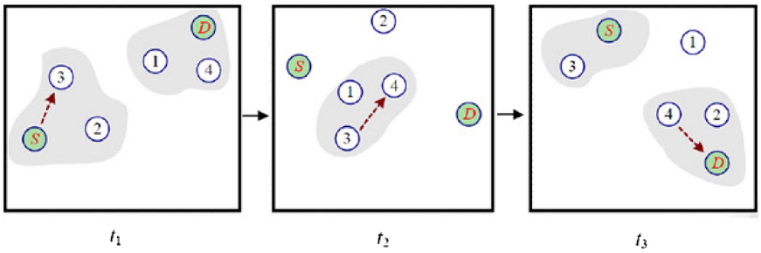


Figure 1 Farmland network environment.

In this paper, Integrated Social Network Routing (SoNR) protocol is modelled behind the movement of cattle in farmland sensor networks. In Figure 1, S could be seen as a calf and D could be seen as it's mother. S might require the location or movement pattern of S for successive time period so that S could rejoin D for some desired purpose. And it is always easier if such S-D pairs are always together, while harvesting the healthcare data [5-7]. In this context, the proposed SoNR protocol would monitor the friends list for misbehaving nodes and it would maintain the friends list only with good reputed friend nodes. Reputation is calculated by (1) Acknowledgement system and (2) Message delivery-based reputation system.

The friends list is periodically updated based on the calculated reputation values. Thus, the updated friends list consists of only good reputed friend nodes, and the message delivery increases gradually as all the nodes in the friends list helps in data forwarding.

2 Related work

Parris and Henderson [8] proposed privacy-enhanced social routing. In this work, two schemes namely statisticulated Social Network Routing (SSNR) and obfuscated Social Network Routing (OSNR) were used. In SSNR, the friends list is modified by adding or removing nodes for each message transmission. Hence, it is not easy for a node to identify the original friends list of a sender by just interpreting a single message. In OSNR, the friends list of source node is embedded in a bloom filter.

Lilien et al. [9] discuss security and privacy challenges in opportunistic networks. The various privacy challenges that need to be considered in oppnet are helper privacy, oppnet privacy, and data privacy. This work discusses the use of trusted devices for more critical tasks, and security routing is enabled by selecting a route that passes through only trusted devices. Alternatively, opportunistic feeding and routing [10] has also been experimented.

Li et al. [11] designed a trust-based framework for data forwarding in opportunistic networks. A watchdog component is included in the trust framework to monitor the behaviour of the forwarding node. The Positive Feedback Message (PFM) is generated by the receiving node to the source to inform the behaviour of the forwarding node. Based on the received PFM, trust to the forwarding behaviour of a node is calculated. The forwarding decision of a

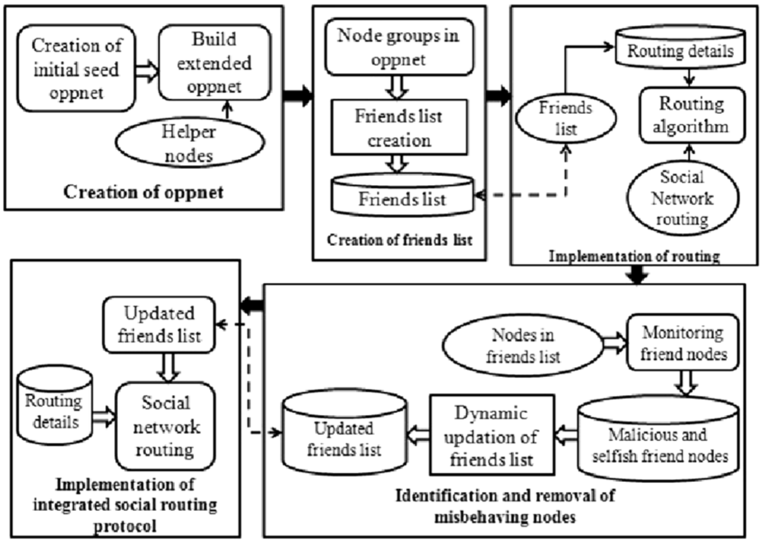


Figure 2 Overall system architecture.

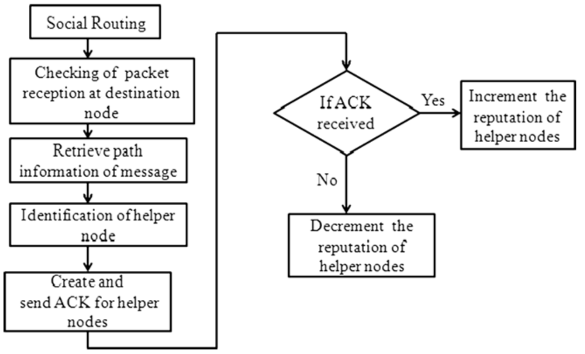

Social Routing
Checking of packet reception at destination node
Retrieve path information of message
Identification of helper node
Create and send ACK for helper nodes
If ACK received
Yes
No
Increment the reputation of helper nodes
Decrement the reputation of helper nodes

Figure 3 Acknowledgement system.

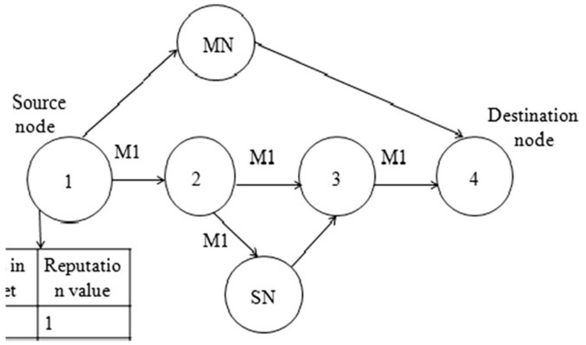


Figure 5 Reputation table updation using ACK system.

node is taken based on the trust and the forwarding ability of a node. Trust-based secured routing models [12,13] concentrating QoS parameters [14] involving artificial intelligence techniques [15] are well addressed in the WSN literature.

Novel reputation computation model based on subjective logic is introduced by Liu et al. [16]. This model identifies and prevents selfish behaviours. This model consists of two phases namely reputation query and reputation computation. In the reputation query phase, a node that receives a service request accumulates the recommended opinions on the requester from their common neighbours who have interacted with it. In the reputation computation phase, node evaluates the reputation with the opinions accumulated in the reputation query phase.

Bigwood et al. [17] proposed a novel incentive mechanism in which self-reported social networks (SRSNs) are used to collect social network data. SRSNs can be obtained from an online social network. These SRSNs are used to provide reputation for nodes. When the network starts up, nodes assign higher trust values to nodes in their SRSN. Selfishness is detected by storing a history of encounter times and exchanging the histories during encounters. Once a node is detected as selfish, the detecting node decrements the value of selfish node by the behaviour constant *x*.

Packet dropping detection scheme and routing misbehaviour mitigation scheme is introduced by Qinghua et al. [18]. In this work, the misbehaviour is monitored and verified by contact record scheme. Every node reports its encountered node with contact records. Any forging in contact records would be identified since there would be inconsistencies in the contact records within the network. The encountered node announces every contact records across the network to at least two witness nodes. Any witness node detecting the inconsistent contact record would report it, and therefore, the misbehaviour shall be identified.

Reputation-based protocol is introduced by Gianluca et al. in [19]. Here, the node with highest reputation is chosen as the next forwarding node. The node list keeps the list of all nodes through which the message has passed through to reach the destination. A node adds itself only once, even though a message passes through that node many times. To avoid malicious nodes from increasing the reputation of other malicious nodes, a list of digital signatures is also attached. This protocol adapts to the changing conditions of DTN and has reduced overhead compared to the existing protocol.

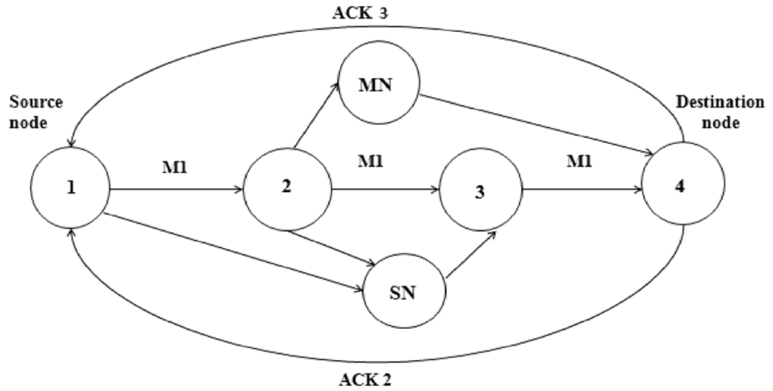
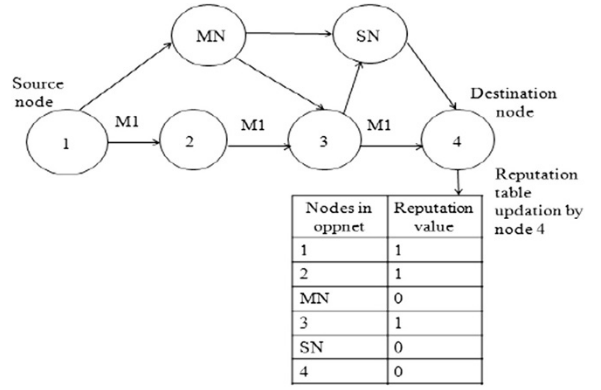


Figure 4 An example of acknowledgement system.



Nodes in oppnet	Reputation value
1	1
2	1
MN	0
3	1
SN	0
4	0

Figure 6 **Reputation table updation using message delivery-based reputation system.**

In addition, few energy-preserving routing protocols do exist for opportunistic networks [20-26]. Location-based routing [27] and directional routing [28] is also experimented for WSNs. Innovative data forwarding methods based on computational geometry [29] have equally been researched so far. The following section briefs the methodology behind the proposed social network-based opportunistic routing for wireless sensor networks (SoNR).

3 Methodology

In the assumed network setup, the nodes may be either fixed or mobile. Different nodes collaborate with each other to exchange data from source to destination. The devices exchange data in a spontaneous manner whenever they come closer. There is no direct connection between source nodes to destination node. A network node discovers its nearest neighbour node, and by using this, it forwards message. Message is delivered hop-by-hop closer to the destination.

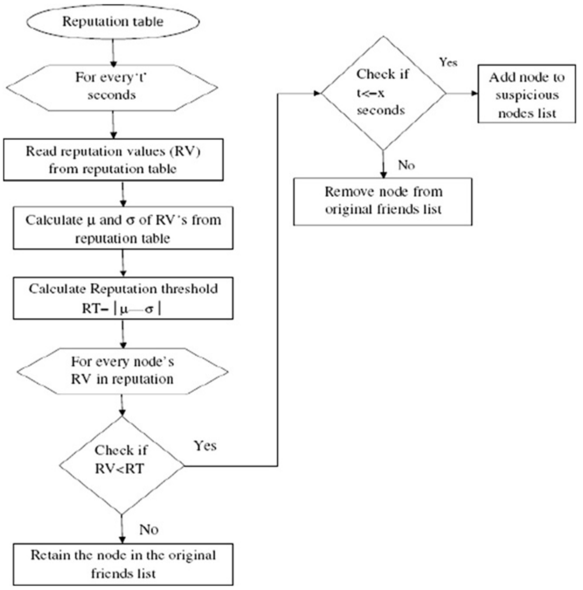

Reputation table
For every 't' seconds
Read reputation values (RV) from reputation table
Calculate μ and σ of RV's from reputation table
Calculate Reputation threshold RT= |μ—σ|
For every node's RV in reputation
Check if RV<RT
Yes
No
Retain the node in the original friends list
Check if t<=x seconds
Yes
Add node to suspicious nodes list
No
Remove node from original friends list

Figure 7 **Threshold-based updation of friends list.**

Figure 2 shows the overall system architecture. The contacts between nodes are viewed as an opportunity to move data closer to the destination. In social network routing, messages are transferred through nodes where the contacts between the nodes are more likely to occur. One such method is forwarding the messages through the friends of source node or destination node. The network consists of group of nodes in which there is a possibility of intruder nodes in some of the groups.

Friends list is created among the good reputation nodes, thus avoiding intruder nodes. But an intruder node in the group can be a friend of another intruder node. A random number generator is used for generating the friends list. The created friends list is stored in a hashmap, where the source node's id is the key for storing its friends list. A node cannot be a friend of itself. An intruder node should not be a friend of a node with good reputation.

Once the friends list is created, messages should be forwarded through the friends in the friends list. For this, the source node first identifies its neighbour nodes. Then, these neighbour nodes are compared with the friends list to identify if any of the neighbour nodes is in the friends list of a source node. If the neighbour node is a friend node of source node, then the messages to the destination is forwarded through this friend node. If the source node meets more than one neighbour friend node, then it forwards the message to all the friend nodes. Hence, the chance of delivering the message to the destination increases.

4 Social network routing

One of the routing techniques available for opportunistic networks is a routing method called epidemic routing [30]. In epidemic routing, messages are routed by flooding the network with copies of messages. Therefore, if a path exists between source and destination, message will certainly be delivered via that path. But sending large numbers of redundant messages is wasteful and will drain the batteries of the sensor nodes rapidly. Though many sensor nodes operate under solar power, a methodology which would not consume much of the energy is ever advisable.

Another main disadvantage of this routing is that the messages are flooded between intruder nodes also. An intruder node will not forward the incoming messages and hence the messages will not reach the destination. Social network routing is one which provides solution to the abovementioned problem.

In social routing, the messages are forwarded through friends of source node or destination node. Friends list is

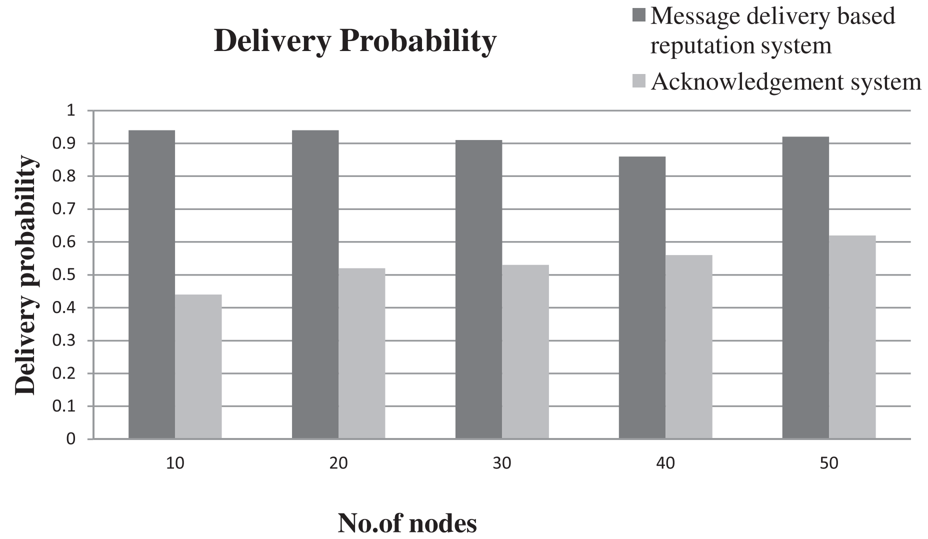


Figure 8 Comparison of message delivery probability by varying the number of nodes.

formed only by using good reputation nodes. Hence, there is no possibility for messages forwarded through intruder nodes. The source node first identifies its neighbour nodes. Then, these neighbour nodes are compared with the friends list to identify if any of the neighbour nodes is in the friends list of a source node. If the neighbour node is a friend node of source node, then the messages to the destination is forwarded through this friend node.

If none of the neighbour node is in the friends list of source node, then the data is stored in the buffer of the source node until it meets the destination node and delivers it once the source node and destination node meets each other. Once the messages in the buffer reach the maximum time to live (TTL) value, they are dropped by the source node. If the incoming message for a node is one which is already in the node's buffer or if there is not enough space for the incoming message, then this node will reject the incoming message. The main advantage of this type of routing is the probability of delivering the data to destination is high.

Social network routing is a protocol in which the messages are forwarded through the friends list of source node or destination node. There is a possibility that the nodes in the friends list might become selfish or malicious in the future. If a friend becomes malicious, then it would drop all the incoming messages to it except for its own destined message. If a friend node becomes selfish, then it would forward the messages only for a short period of time, and after sometime, it would start dropping all the incoming messages except for its own destined message. Hence, it is necessary to monitor all the nodes in the friends list.

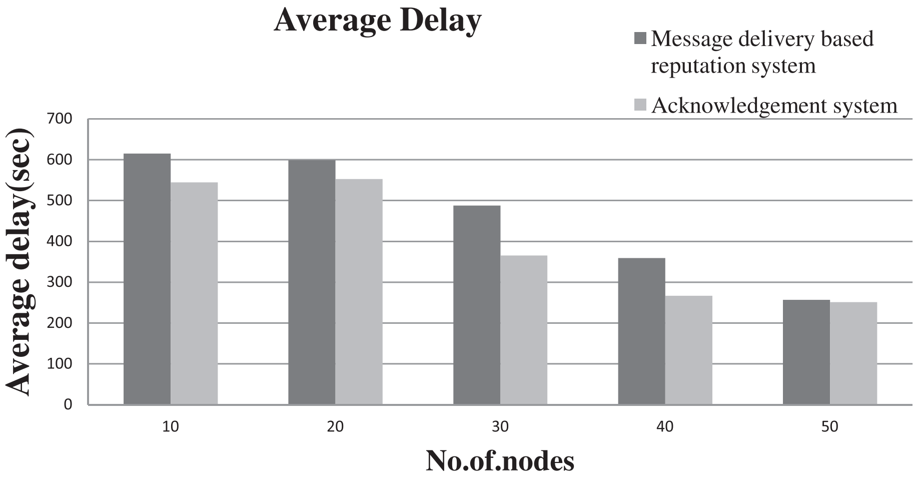


Figure 9 Comparison of average delay by varying the number of nodes.

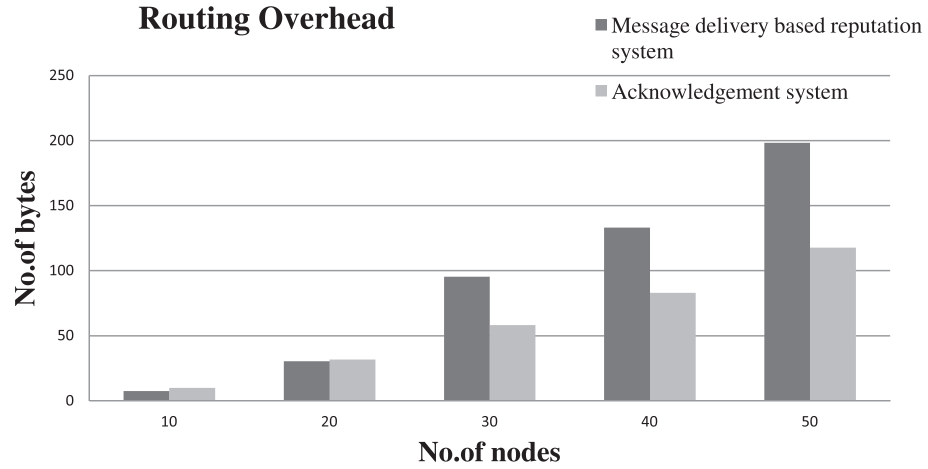


Figure 10 **Comparison of routing overhead by varying the number of nodes.**

In this paper, we propose the integrated social network routing protocol in which the friends list is monitored periodically for identifying the misbehaving nodes in the friends list. Once the misbehaving nodes are identified, they are removed from the friends list and the friends list is updated only with good reputed friend nodes.

The integrated social network routing protocol calculates the reputation of all the nodes in the network and maintains the reputation values in a reputation table. It uses two methodologies for calculating the reputation of nodes in the network, namely (1) acknowledgement system and (2) message delivery-based reputation system.

In the acknowledgement system, the destination node creates the ACK messages for each helper node which helped for transmitting its own destined message to it. It sends the created ACK to the source node of the message, and if the source node receives the ACK, it would increment the reputation of the helper nodes. In message delivery-based reputation system, the destination node will directly increment the reputation of helper nodes in the reputation table.

The reputation values in the reputation table are periodically analyzed, and the reputation threshold (RT) is calculated. Then the reputation (R) of all the nodes is compared with this reputation threshold, and if any node's reputation value is less than the reputation threshold, then the node is identified as misbehaving node. However, the misbehaving node thus identified is not immediately removed from the friends list, but is added to a list of suspicious nodes. And if a node remains in the suspicious nodes list for a long time, it is removed from the friends list. Then, the updated friends list consists of only good reputed friend nodes and ensures good delivery rate of messages.

5 Reputation calculation using acknowledgement system

In Figure 3, the acknowledgement system is shown. In this system, after each message is received at the destination, the destination node finds the nodes which helped for forwarding the messages to it. The destination node uses the path information for finding the helper nodes.

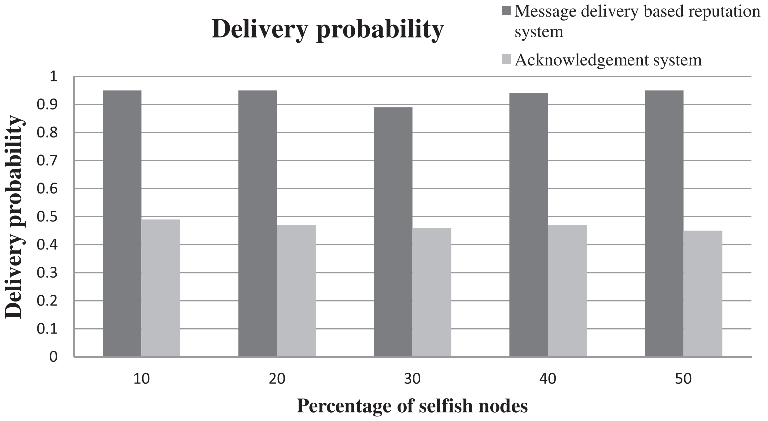


Figure 11 **Comparison of message delivery probability by varying the percentage of selfish nodes.**

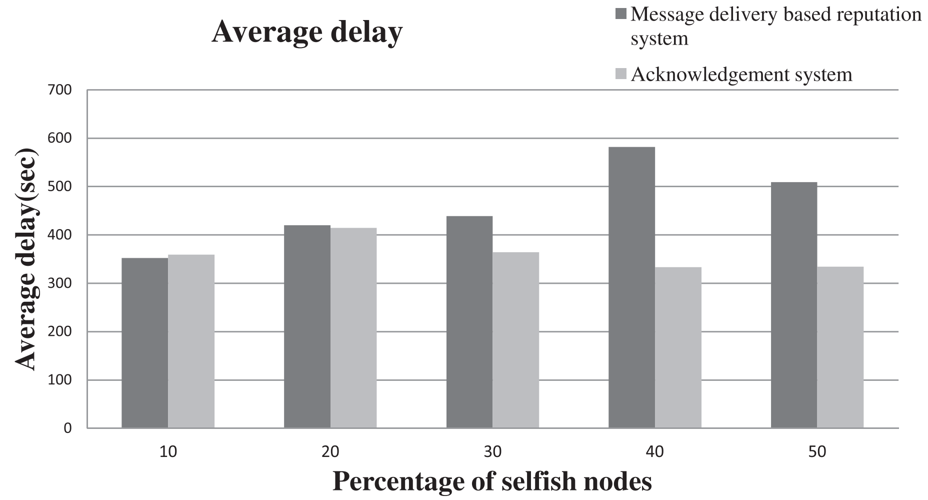


Figure 12 Comparison of average delay by varying the percentage of selfish nodes.

Then, it creates and sends ACK message for the helper nodes to the sender node of the message. Once the sender node receives ACK message of the helper nodes, it increments the reputation value of the helper nodes.

In Figure 4, node 1 generates message M1 and sends to node 4. Message M1 is transmitted to node 2. The node 2 then forwards the message to node 3, node MN and node SN. Here, node MN is a malicious node and hence drops the message M1, and the node SN is a selfish node, which would keep the message for some time in its buffer and later drops the message without forwarding it to destination node. Hence, the node 3 alone helps in forwarding the message to the destination node. Thus, the reputation value is incremented only for node 3, and the reputation values for nodes MN and SN remain the same.

Figure 5 shows the updation of reputation values by the source node after receiving the ACK messages of the helper nodes from the destination node. In Figure 5, the reputation values of nodes 1, 2, and 3 are incremented as they helped for forwarding the data whereas the reputation values of nodes MN and SN are the same as they dropped the messages without forwarding it to the destination node.

6 Reputation calculation using message delivery-based reputation system

This system also creates and initializes the reputation table for updating the reputation values of the nodes. In this system after the destination node receives message, it finds the nodes which helps in transmitting the messages to it. The destination node uses the path information for finding the helper nodes, and then, it directly increments the reputation values of those nodes which helps in transmitting the messages to it.

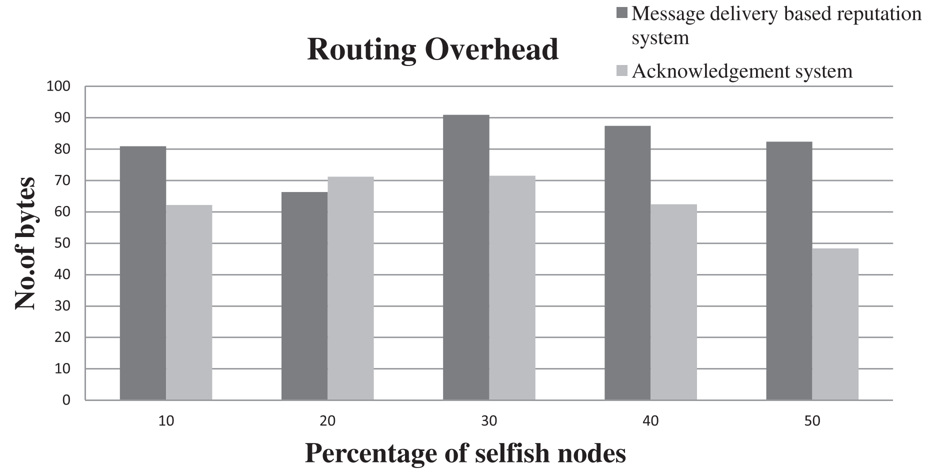


Figure 13 Comparison of routing overhead by varying the percentage of selfish nodes.

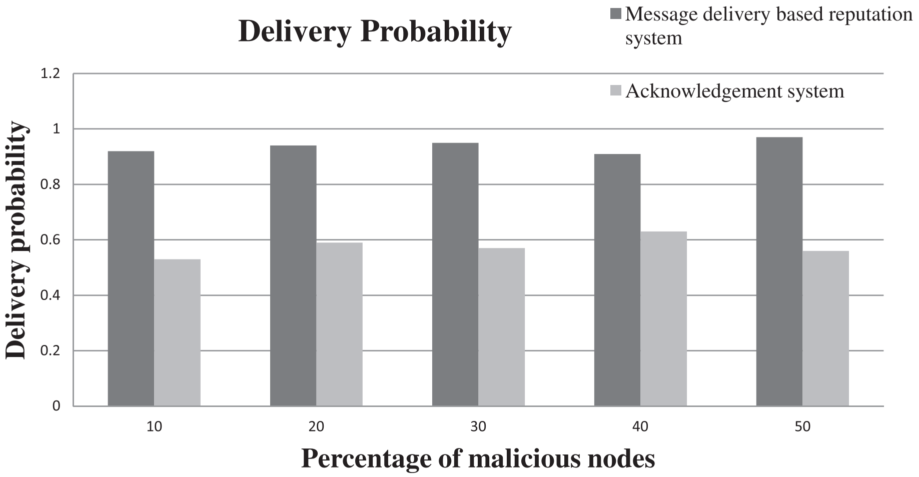


Figure 14 Comparison of message delivery probability by varying the percentage of malicious nodes.

From Figure 6, we can see that the message M1 is transmitted from source node 1. The source node then forwards the message to node 2 and node MN. The node 2 alone forwards the message to node 3, but the node MN drops the message M1. The node 3 after receiving message forwards M1 to node 4 and node SN. The node SN put the message in its buffer and drops it after some period of time. Here, node 4 is the destination node and hence receives its message from node 3. Once the destination node receives the message, it would retrieve the path information for message M1. Then, it finds the node which helped in forwarding the message for it using the path information. From Figure 6, it is seen that the destination node directly updates the reputation values of the helper nodes in the reputation table, whereas in the ACK system, the source node updates the reputation table.

Algorithm to update message delivery based reputation system is:

```
1. Begin
2. Initialize the reputation values of all the nodes in the
   network
3. If the message (M) reaches the destination node (D),
   then 'D'
   i. Retrieves the path information of the received message
   ii. Identifies the helper nodes from path [] of the
       message M)
   iii. Increments the reputation values of the helper nodes
4. End
```

7 Threshold-based updation of friends list

The flow diagram for threshold-based updation of friends list is shown in Figure 7. The friends list is updated at

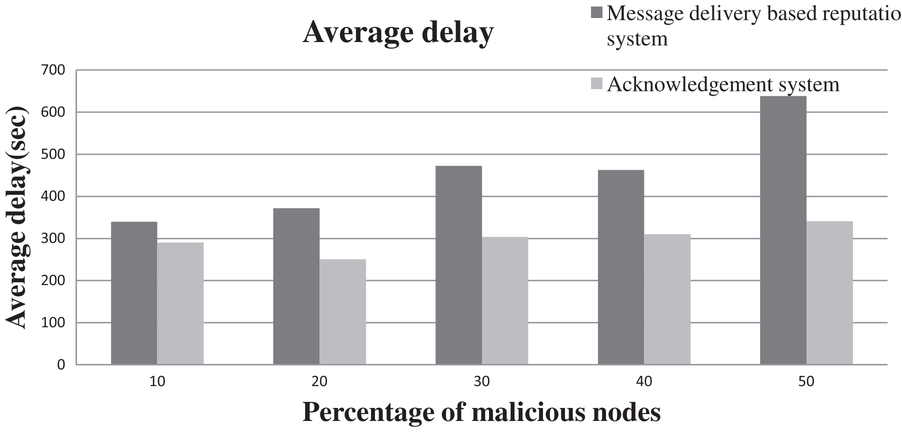


Figure 15 Comparison of average delay by varying the percentage of malicious nodes.

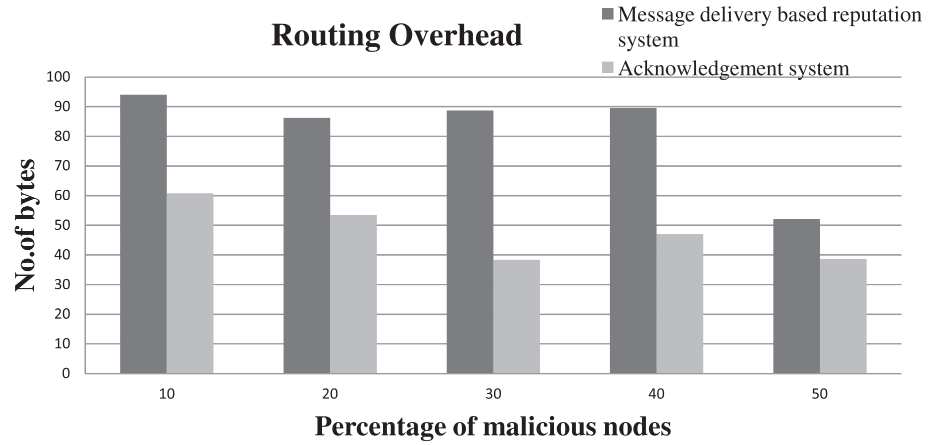


Figure 16 Comparison of routing overhead by varying the percentage of malicious nodes.

regular time interval of every 1,000 seconds. The reputation values for all the nodes is calculated and maintained in the reputation table for every delivered message using the two methodologies namely ACK system and message delivery-based reputation system. For updating the friends list, first, the mean (μ) and standard deviation (σ) of reputation values from the reputation table is calculated. Then, the reputation threshold (RT) = $\left| \mu - \sigma \right|$ is calculated. The reputation value of all the nodes is compared with the calculated reputation threshold, and if the reputation value of a node is less than the calculated threshold, then that node is added to suspicious list of nodes. If the node remains in the suspicious list of nodes for a long time, then that node is identified as a misbehaving node and is removed from the friends list. Hence, after certain period of time, the friends list consists of only good reputed friend nodes.

8 Results

The following parameters are considered for the assessment of integrated social network routing protocol.

- Delivery probability - maximum probability to deliver the message successfully.
- Overhead - additional bytes relayed to ensure packet delivery with maximum probability.
- Average delay - the duration between the message's generation time and the message's delivery time.
- False negative - if a misbehaving node is classified as a good node, then it a false negative.
- False negative - if a misbehaving node is classified as a good node, then it a false negative.
- Classification accuracy - accuracy of a measurement system is the degree of closeness of measurements of a quality to that quantity's actual (true) value.

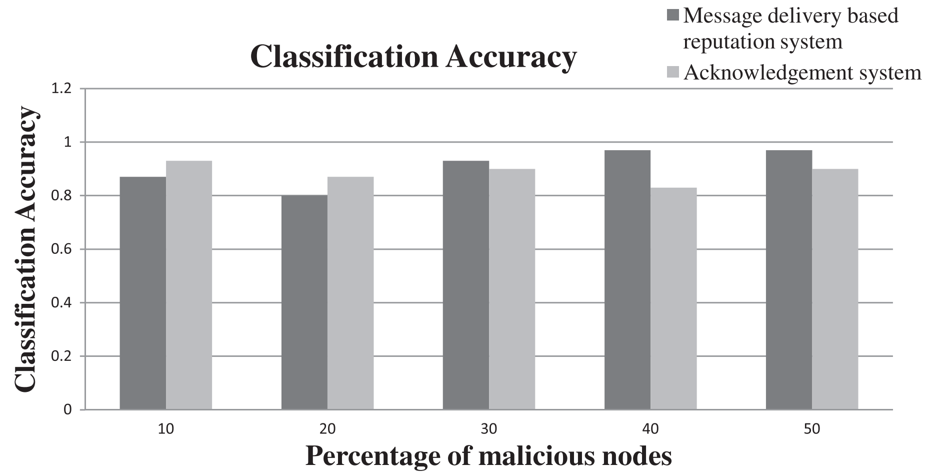


Figure 17 Comparison of classification accuracy by varying the percentage of malicious nodes.

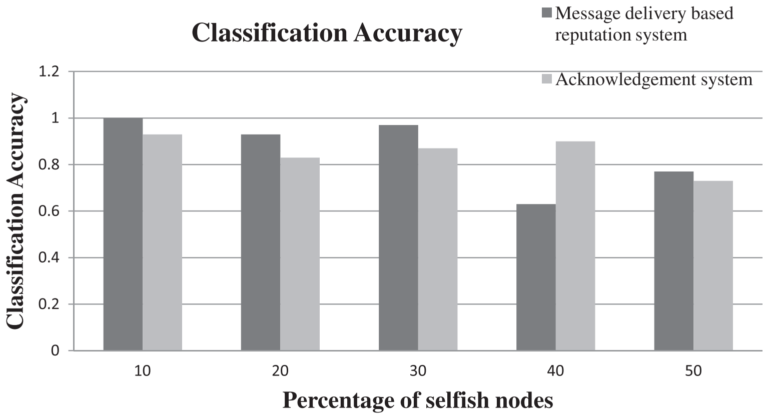


Figure 18 **Comparison of classification accuracy by varying the percentage of selfish nodes.**

Figure 8 shows the comparison of message delivery probability of SoNR under message delivery-based reputation system and ACK system by varying number of nodes and keeping the number of malicious and selfish nodes as constant. It shows that the delivery probability is very high for message delivery-based reputation system. The acknowledgement system updates the reputation table based on the received ACK. If the ACK is not received for a node, then the reputation value is not incremented even though the node helps for transmitting a message whereas in the message delivery-based reputation system, the reputation table is directly updated by the destination node for those nodes which helps for transmitting the messages to it. Hence, all the good nodes are involved in message transmission in this messages delivery-based reputation system, and therefore, the reputation probability is high for this system.

Figure 9 shows the comparison of average delay for message transfer of SoNR under the message delivery-based reputation system and ACK system by varying the number of nodes and keeping the number of malicious and selfish nodes as constant. The average delay for message transfer decreases when the number of nodes is increased for both acknowledgement system and message delivery-based reputation system when the node density is high. This is because if the node density is high, then there is a frequent chance for the transmitting node to meet its friend node and hence the message is delivered very soon to its destination.

Figure 10 shows the comparison of routing overhead of SoNR under the message delivery-based reputation system and ACK system while varying the number of nodes and keeping the number of malicious and selfish nodes as constant. The result shows that the additional information required to route message successfully increases when the node density increases for both message delivery-based reputation system and ACK system. This is because if the node density increases, then the additional information required to route the messages also increases.

Figure 11 shows the comparison of message delivery probability of SoNR under message delivery-based reputation system and ACK system by varying percentage of selfish nodes and keeping the number of malicious nodes and number of nodes as constant. It is seen

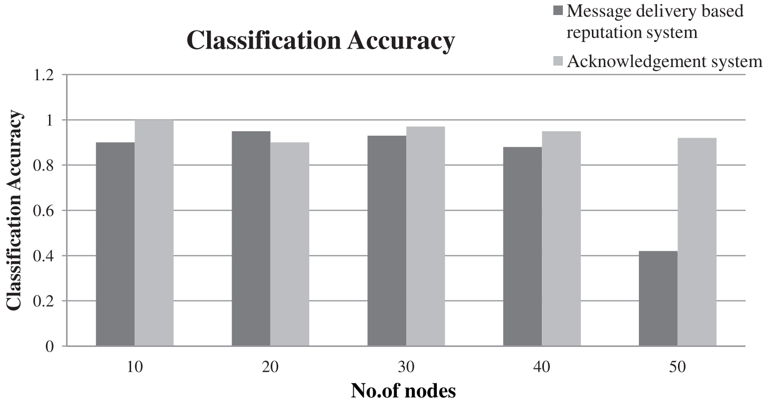


Figure 19 **Comparison of classification accuracy by varying the number of nodes.**

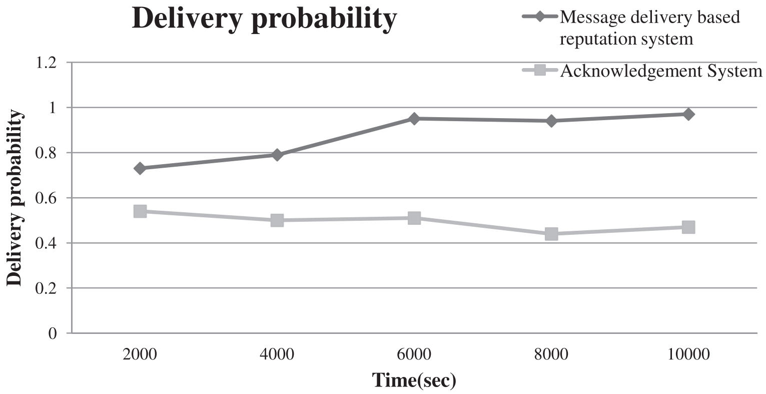


Figure 20 Comparison of delivery probability by varying time.

from the figure that the delivery probability remains high for message delivery-based reputation system even if the percentage of selfish nodes is very high because this SoNR protocol correctly identifies these selfish nodes in the friends list and removes them. Thus, the friends list consists of only good reputed friend nodes which help in transmitting the messages successfully to the destination.

Figure 12 shows the comparison of average delay of SoNR protocol under the message delivery-based reputation system and ACK system by varying the percentage of selfish nodes and keeping the number of malicious nodes and number of nodes (30) as constant. It shows that there is high delay for both the systems. The delay is high because of the high density of selfish nodes in the network.

Figure 13 shows the comparison of routing overhead of SoNR protocol under the message delivery-based reputation system and ACK system while varying the percentage of selfish nodes and keeping the number of malicious nodes and number of nodes (30) as constant. The result shows that the additional information required to route message successfully increases when the node density increases for both message delivery-based system compared to that of ACK system. This is because if the node density increases, then the additional information required to route the message also increases.

Figure 14 shows the comparison of message delivery probability of SoNR protocol under message delivery-based reputation system and ACK system by varying the percentage of malicious nodes and keeping the number of selfish nodes and number of nodes (30) as constant. It is seen from the figure that the delivery probability remains high for message delivery-based system even if the percentage of malicious nodes is very high because this SoNR protocol correctly identifies these malicious nodes in the friends list and remove them. Thus, the friends list consists of only good reputed friend nodes which help in transmitting the messages successfully to the destination.

Figure 15 shows the comparison of average delay of SoNR under the message delivery-based system and ACK system by varying the percentage of malicious nodes. The figure shows that there is high delay for both the systems.

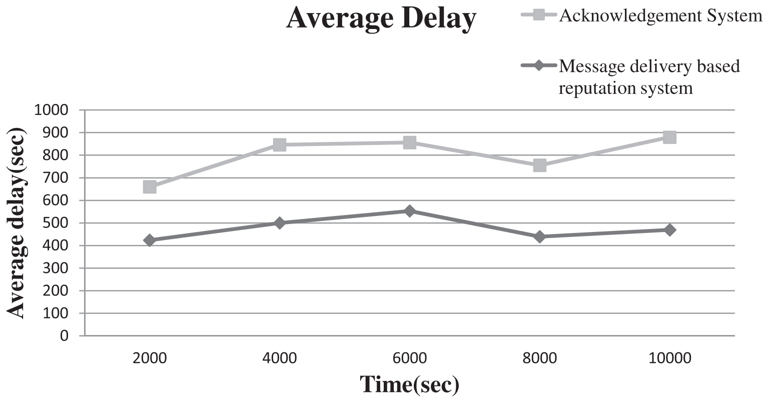


Figure 21 Comparison of average delay by varying time.

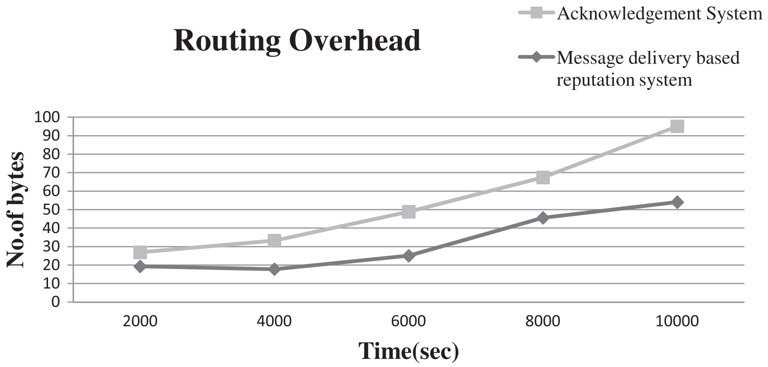


Figure 22 Comparison of routing overhead by varying time.

The delay is high because of the high density of malicious nodes in the network.

Figure 16 shows the comparison of routing overhead of SoNR protocol under the message delivery-based system and ACK system while varying the percentage of malicious nodes in the network. The result shows that the additional information required to route message successfully increases when the node density increases for both message delivery-based system compared to that of ACK system. This is because if the node density increases, then the additional information required to route the message also increases.

Figure 17 shows the classification accuracy of SoNR protocol under message delivery-based reputation system and ACK system by varying the percentage of malicious nodes in the network. The number of nodes (30) and the number of selfish nodes are kept as constant. It shows that the classification accuracy is high for both message delivery-based system and acknowledgement system. This is because the false negatives are very less for both the systems and the false positives are high compared to false negatives. Hence, these figures shows that all the bad nodes are correctly classified, and some of the good nodes are classified as bad nodes.

Figure 18 shows the comparison of classification accuracy of SoNR protocol under message delivery-based reputation system and ACK system by varying the percentage of selfish nodes and keeping the number of malicious nodes and number of nodes (30) as constant. The classification accuracy in Figure 18 is lower than in that in Figure 17 since there are more false negatives than false positives, and hence, the classification accuracy is reduced.

Figure 19 shows the classification accuracy of SoNR protocol under message delivery-based reputation system and ACK system by varying the number of nodes and keeping the number of malicious nodes and number of nodes (30) as constant. The false negatives and false positives are very less for acknowledgement system when compared to that of the message-delivery based system. Hence, the classification accuracy is high for ACK system when compared to that of the message delivery-based reputation system.

The comparison of message delivery probability of SoNR protocol under message delivery-based reputation system

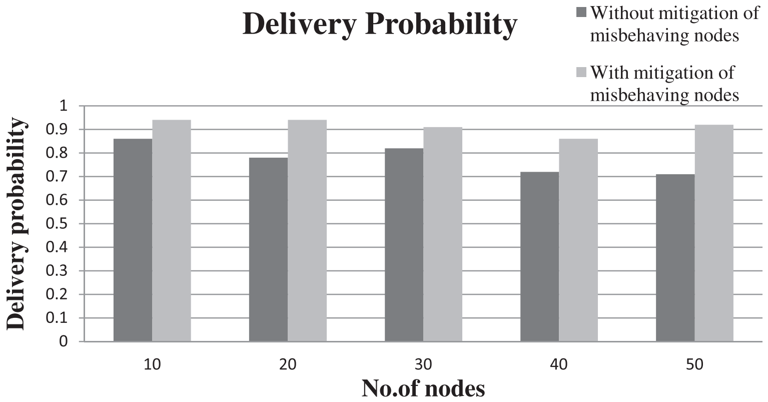


Figure 23 Comparison of message delivery probability of message delivery-based reputation system by varying the number of nodes.

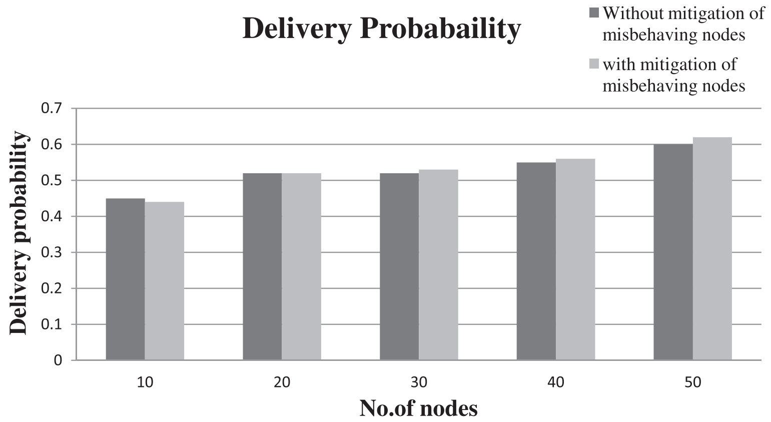


Figure 24 Comparison of message delivery probability of acknowledgement system by varying the number of nodes.

and ACK system by varying time is shown in Figure 20. It is seen from the figure that the message delivery probability of message delivery-based reputation system increases when time increases.

The comparison of average delay of SoNR protocol under message delivery-based reputation system and ACK system by varying time is shown in Figure 21. The figure shows that the delay increases for ACK system when time is increased. This is because all the nodes need to transfer the messages as well as the ACK message. The comparison of routing overhead of SoNR protocol under message delivery-based reputation system and ACK system by varying time is shown in Figure 22. It is seen from the figure that the routing overhead is increased when the time increases. This is because when the time increases, the additional byte to transfer the message successfully also increases.

The comparison of message delivery probability of SoNR protocol under message delivery-based reputation system by varying number of nodes is shown in Figure 23. The comparison of message delivery probability of SoNR protocol under ACK system by varying the number of nodes is shown in Figure 24. It is seen that the delivery probability is high when the misbehaving nodes are mitigated.

In a nutshell, message delivery-based reputation system performs much better than acknowledgement system. Table 1 provides a comparison of the proposed protocol with that of the standard AODV and DSR protocols. The packet delivery ratio is higher in both the variations of SoNR which shows the power of social network routing.

Table 1 Evaluation of the proposed protocol with AODV and DSR – with 50% malicious nodes

	Proposed SoNR (Ack)	Proposed SoNR (Rep)	AODV	DSR
Packet Delivery Ratio	0.58	0.98	0.52	0.31
Throughput (kbps)	3.86	6.38	4.9	2.86
Routing Overhead %	39	52	62.2	41.3

The reputation-based SoNR shows significant reduction in routing overhead since AODV and DSR are less efficient in identifying the presence of malicious nodes and are less capable for malicious node-aware effective data forwarding. Subbaraj et al [31] support the above claim that the standard AODV and DSR protocols require trust and reputation support for handling routing in the presence of malicious nodes.

9 Conclusions

This research mainly focused on integrated social network routing (SoNR) protocol which routes the messages only through good reputed friend nodes. Simulation results show that the delivery probability of message delivery-based reputation system of integrated social network routing protocol is 30% better when compared to that of the acknowledgement system of integrated social network routing protocol. The percentage of classifying bad nodes as good nodes is very less. However, the present work does not consider the collusion of malicious and selfish nodes.

Competing interests

The authors declare that they have no competing interests.

Author details
[1]Department of Computer Science and Engineering, Sri Lakshmi Ammal Engineering College, Thiruvanchery, Tambaram East, Chennai 600126, India. [2]Department of Computer Science and Engineering, Thangavelu Engineering College, Rajiv Gandhi Salai, Karapakkam, Chennai 600097, India.

Received: 26 June 2014 Accepted: 19 August 2014
Published: 28 August 2014

References

1. M Li, L Zhenjiang, AV Vasilakos, A survey on topology control in wireless sensor networks: taxonomy, comparative study, and open issues. Proc. IEEE **101**(12), 1–20 (2013)

2. A Vasilakos, MP Saltouros, AF Atlassis, W Pedrycz, *Optimizing QoS routing in hierarchical ATM networks using computational intelligence techniques*. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 33, vol. 3, 2003, pp. 297–312
3. T Spyropoulos, RN Rais, T Turletti, K Obraczka, A Vasilakos, Routing for disruption tolerant networks: taxonomy and design. Wirel. Netw **16**(8), 2349–2370 (2010)
4. AV Vasilakos, Y Zhang, T Spyropoulos (eds.), *Delay Tolerant Networks: Protocols and Applications* (CRC Press, 2012)
5. Y Yao, Q Cao, AV Vasilakos, *EDAL: An Energy-Efficient, Delay-Aware, and Lifetime-Balancing Data Collection Protocol for Wireless Sensor Networks*. IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS), 2013, pp. 182–190
6. K Han, J Luo, Y Liu, AV Vasilakos, Algorithm design for data communications in duty-cycled wireless sensor networks: a survey, communications magazine. IEEE **7**, 51 (2013)
7. G Acampora, DJ Cook, P Rashidi, AV Vasilakos, A survey on ambient intelligence in healthcare. Proc. IEEE **101**(12), 1–25 (2013)
8. I Parris, T Henderson, *Privacy-Enhanced Social Network Routing, Computer Communications*, vol. 1, 35th edn. (Elsevier, 2012), pp. 62–74
9. L Lilien, ZH Kamal, V Bhuse, A Gupta, The concept of opportunistic networks and their research challenges in privacy and security. Mobile Wireless Network Secur. Privacy 85–117 (2007)
10. P Li, S Guo, S Yu, AV Vasilakos, CodePipe: an opportunistic feeding and routing protocol for reliable multicast with pipelined network coding, INFOCOM. Proc. IEEE **108**, 100–108 (2012)
11. N Li, SK Das, A trust-based framework for data forwarding in opportunistic networks. Ad Hoc Netw. **11**(4), 1497–1509 (2013)
12. D He, C Chen, S Chan, J Bu, AV Vasilakos, ReTrust: attack-resistant and lightweight trust management for medical sensor networks. IEEE Trans. Inf. Technol. Biomed. **16**(4), 623–632 (2012)
13. D He, C Chen, S Chan, J Bu, AV Vasilakos, A distributed trust evaluation model and its application scenarios for medical sensor networks. Inf. Technol. Biomed. IEEE Trans. **16**(6), 1164–1175 (2012)
14. S Zhengguo, S Yang, Y Yu, AV Vasilakos, JA McCann, KK Leung, A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. Wireless Commun. IEEE **20**(6), 91–98 (2013)
15. Y Moustafa, M Ibrahim, M Abdelatif, L Chen, A Vasilakos, *Routing Metrics of Cognitive Radio Networks: A Survey*, 2013, pp. 1–18
16. Y Liu, K Li, Y Jin, Y Zhang, W Qu, A novel reputation computation model based on subjective logic for mobile ad hoc networks. Futur. Gener. Comput. Syst. **27**(5), 547–554 (2011)
17. G Bigwood, T Henderson, *IRONMAN: Using Social Networks to Add Incentives and Reputation to Opportunistic Networks, Rivacy, Security, Risk And Trust (Passat)*. 2011 IEEE third international conference on and 2011 ieee third international conference on social computing (socialcom) (IEEE, MIT, Boston, USA, 2011), pp. 65–72
18. Q Li, G Cao, Mitigating routing misbehavior in disruption tolerant networks. Inf. Forensics Secur. IEEE Trans. **7**(2), 64–675 (2012)
19. G Dini, A Lo Duca, Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network. Ad Hoc Netw. **10**(7), 1167–1178 (2012)
20. I Ahmedy, MA Ngadi, SN Omar, Using store-forward technique to conserve energy in wireless sensor networks: initial step for routing mechanism, Computing Technology and Information Management (ICCM). 8th Int Conf **2**(1), 671–676 (2012)
21. S Chelloug, M Benmohammed, *Simulated Annealing for Maximizing the Lifetime of Sensor Networks under Opportunistic Routing, Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications* (IEEE Computer Society, Canada, 2012), pp. 14–19
22. C Wei, C Zhi, P Fan, KB Letaief, AsOR: an energy efficient multi-hop opportunistic routing protocol for wireless sensor networks over Rayleigh fading channels. Wireless Commun. IEEE Trans. **8**(5), 2452–2463 (2009)
23. M Kaliszan, S Stanczak, *Maximizing Lifetime in Wireless Sensor Networks Under Opportunistic Routing, Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference* (IEEE, California, USA, 2010), pp. 1913–1917
24. ME Rusli, R Harris, A Punchihewa, Quality aware opportunistic routing protocol with adaptive coordination scheme for wireless sensor networks, in *Computational Intelligence, Modelling and Simulation (CIMSiM), 2012 Fourth International Conference* (IEEE, Malaysia, 2012), pp. 434–439
25. ME Rusli, R Harris, A Punchihewa, Performance analysis of implicit acknowledgement coordination scheme for opportunistic routing in wireless sensor networks, in *Telecommunication Technologies (ISTT), 2012 International Symposium* (IEEE, Malaysia, 2012), pp. 131–136
26. JM Soares, RM Rocha, CHARON: routing in low-density opportunistic wireless sensor networks, in *Wireless Days (WD), 2009 2nd IFIP* (IEEE, Paris, 2009), pp. 1–5
27. Y Han, Z Lin, A geographically opportunistic routing protocol used in mobile wireless sensor networks, in *Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference* (IEEE, Beijing, 2012), pp. 216–221
28. Y Zeng, K Xiang, D Li, AV Vasilakos, Directional routing and scheduling for green vehicular delay tolerant networks. Wirel. Netw **19**(2), 161–173 (2013)
29. J Luo, Y Cai, A data forwarding scheme based on delaunay triangulation for CPSs, in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference* (IEEE, China, 2012), pp. 1–6
30. SK Tan, A Munro, Adaptive probabilistic epidemic protocol for wireless sensor networks in an urban environment, in *Computer Communications and Networks, 2007. ICCCN 2007*. Proceedings of 16th International Conference (IEEE, 2007), pp. 1105–1110
31. S Subbaraj, S Prakash, EigenTrust-based non-cooperative game model assisting ACO look-ahead secure routing against selfishness. Eurasip J. Wirel. Commun. Netw. **2014**(1), 78 (2014)

doi:10.1186/1687-1499-2014-141
Cite this article as: Shobana and Narayanasamy: **Integrated social network reputation inspired routing for effective data forwarding.** *EURASIP Journal on Wireless Communications and Networking* 2014 **2014**:141.