EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique

Senthilkumar Subramaniyan[1*], William Johnson[2] and Karthikeyan Subramaniyan[3]

Abstract

A mobile *ad hoc* network (MANET) is a self-organized system comprised by multiple mobile wireless nodes. The node misbehavior due to selfish reasons can significantly diminish the performance of MANET. A selfish node attempts to use the resources only for its own purpose and it hesitates to share the resources with their neighbors. So, it is very important to detect the selfish nodes to improve the performance of MANET. Initially, an architectural model of a MANET is constructed and the communication between the mobile is originated. The packet drop can happen in MANET due to the selfish node or network congestion. In this paper, a Record- and Trust-Based Detection (RTBD) technique is proposed to detect the selfish nodes efficiently in MANET. The main reason for using trust in this analysis is to accelerate the detection of misbehaving nodes. This study has been carried out in order to analyze the detection of selfish nodes on essential network functions such as routing and packet dropping. The results show that the proposed selfish node detection method is very efficient, since the detection time of selfish nodes is diminished and the overall overhead is very low. The simulation study demonstrates that the proposed RTBD method enhances the selfish node detection ratio, packet delivery ratio (PDR), and average packet drop ratio.

Keywords: Mobile *ad hoc* network (MANET); Selfish node; Record- and Trust-Based Detection (RTBD); Route discovery; Route request (RREQ); Packet delivery ratio (PDR)

1 Introduction

Mobile *ad hoc* network (MANET) is a wireless network among mobile devices. It is a self-configuring system of mobile nodes connected by wireless links, which contains a network area with nodes. This network is relatively a new communication paradigm, which contains a group of mobile devices communicating through a wireless medium. A major problem in MANETs is the frequent occurrence of network divisions due to the unlimited movement of the mobile nodes in the network. This results in some data getting inaccessible to some of the nodes. Thus, data accessibility needs to be considered carefully in MANET [1]. Each mobile node in MANET requires the help of other nodes to forward the packets. The nodes are expected to wait for a pre-defined time interval between successive transmissions. But a mobile node may misbehave due to network congestion and selfishness. Node misbehavior due to selfish or malicious reasons or faulty nodes can significantly reduce the performance of MANETs.

Node misbehavior means deviation from the original routing and forwarding. The source node can relay packets to the destination node through other nodes in MANET. The selfish nodes [2] do not participate in the routing process, which intentionally delay and drop the packet. These misbehaviors of the selfish nodes will impact the efficiency, reliability, and the fairness. A selfish node does not perform the process related to packet forwarding function for data packets unrelated to itself. The selfish node utilizes its limited resources only for its own purpose because of the energy and storage constraints for each node in the MANET. It aims to save its resources to the maximum, so this type of misbehaving node discards all incoming packets except those which are destined to it. The selfish nodes neglect to share their resources, such as battery power, CPU time, and memory space to other

* Correspondence: senthilkumarphd2013@gmail.com
[1]Department of Computer Science and Engineering, University College of Engineering Pattukottai, Tamil Nadu 614701, India
Full list of author information is available at the end of the article

nodes in MANET. This behavior is observed in the data link/MAC layer, which is decisive, specifically when the mobile nodes possess small residual power.

The features of the selfish nodes are as follows:

- Non-participation in routing
- No transmission or reply to HELLO messages
- Intentional postponement of route request (RREQ) packets
- Data packet dropping

Managing trust [3] in a distributed MANET is a challenging and critical task to achieving mission and system goals such as reliability, scalability, availability, and reconfigurability. Trust management contributes a unified approach for interpreting and specifying security policies, credentials, and relationships. It involves [4] trust establishment, trust revocation, and trust update in MANET. The trustworthiness is evaluated using the trust information or evidence, which is difficult due to changes in topology induced by node mobility or node failure. In this MANET framework, the nodes are connected to the network, which are monitored by a server agent, and the MANET architecture is shown in Figure 1. It manages the details of the mobile nodes in a network like

- Behavior of the node
- Speed of the node
- Direction of the node
- Position of the node

The main objective of the proposed work is to detect the selfish node in MANET using the Record- and Trust-Based Detection (RTBD) technique. The proposed method consists of a packet dropping detection scheme and a selfish node mitigation scheme. The selfish node is required to generate a trust report during each neighbor, which reports its previous communication reports to the neighboring node. Based on that report, the neighboring node detects if the selfish node has dropped packets. The neighboring node gathers the trust report to detect misreporting and then it finds out which node has dropped packets. A selfish node may report a false record to hide the dropping from being detected.

The remaining part of the paper is organized as follows: Section 2 involves the works related to existing solutions for handling and detecting the selfish nodes in MANET. Section 3 involves the description of the RTBD method - selfish node detection based on trust reports and packet drop rates. Section 4 involves the performance evaluation and comparison of selfish node detection based on trust reports and packet drop rates and existing techniques based on trust. Section 5 concludes the paper and identifies the future research directions.

2 Related work

This section deals with the existing solutions for handling and detecting the nodal misbehavior in MANET. Singh et al. [5] implemented a security-based algorithmic

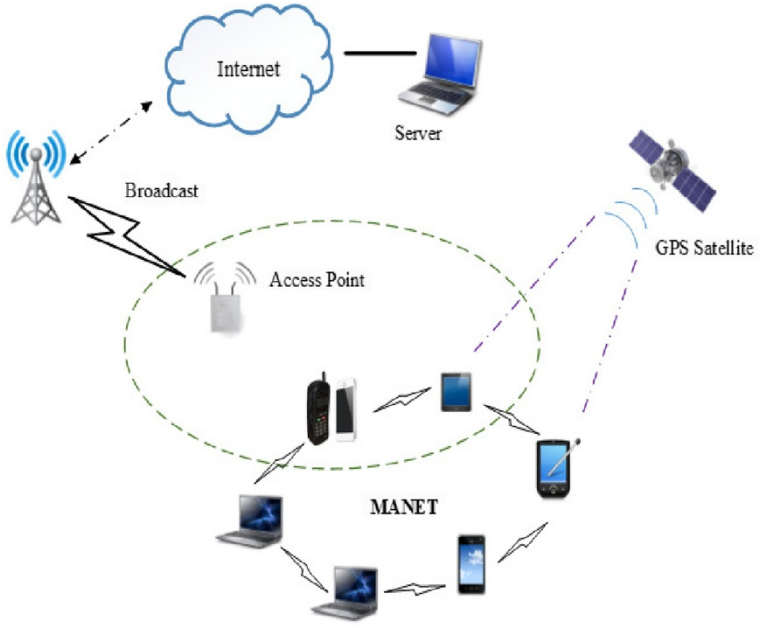

Figure 1 Basic MANET architecture.

approach in MANETs. In this analysis, an empirical and effective approach was proposed to optimize the packet loss frequency. Hernandez et al. [6] introduced a fast model to evaluate the selfish node detection in MANET using a watchdog approach. They estimated the time of detection and the overhead of collaborative watchdog approach for detecting one selfish node. Manoj et al. [7] introduced a novel trust-based certificate authority concept to transmit data packets through trusted nodes and insulates malicious nodes in MANET. The suggested trust management scheme provides low battery power consumption and packet integrity aspect in addition to direct and indirect trust values. Jawhar et al. suggested a reliable routing protocol for enhanced reliability and security of communication in the MANET and sensor networks [8]. In this paper, the reliability and security were achieved by the maintenance of a reliability factor by the nodes. Rodriguez and Gozalvez [9] recommended a reputation-based selfishness prevention technique for MANET. Disparate reputation-based protocols were proposed in this paper to observe the correct relaying of packets and to compile information about potential selfish nodes.

Afghah et al. [10] suggested a unique game theoretical method to model packet forwarding in relay networks. In this paper, a stationary Markovian model was utilized to optimize the system performance in terms of throughput, delay, and power consumption cost. Hernandez et al. [11] endorsed a collaborative watchdog approach to improve the selfish node detection in MANETs. They introduced an analytical method to evaluate the selfish node detection time and the cost of the collaborative approach. Padiya et al. suggested an innovated technique to detect selfish nodes in MANET [12]. The authors discussed three techniques to detect selfish nodes in MANET, namely reputation-based technique, credit-based technique, and acknowledgement-based technique. It was beneficial only for a node not to send the alarm message to avoid the risk. Roy and Chaki [13] designed a new intrusion detection system (IDS) based on mobile agents. The intent of this analysis was to address the limitations of IDS systems by taking advantage of the mobile agent system. Koshti and Kamoji [14] described two techniques, namely reputation-based system and credit-based system, for detecting selfish nodes in MANET. In this study, the 2ack scheme was used to detect and mitigate the effect of misbehaving nodes in MANET.

Patil and Kallimath [15] implemented a cross-layer approach for detecting selfish nodes in MANET. The main aim of this paper was to enhance the routing in MANET by using on-demand routing protocols such as *ad hoc* on-demand distance vector (AODV) routing protocol. Kurkure and Chaudhari [16] illustrated a comparative analysis of the selfish node detection methods based on detection time and message overhead. In this paper, a collaborative watchdog method was used to identify the selfish nodes and diminish the detection time and message overhead. Nandhini et al. [17] implemented an effective ant-based routing algorithm to diminish the overhead in a mobile network. The authors proposed a novel approach based on an ant colony algorithm to enhance the efficiency and to diminish the overhead. Ciobanu et al. [18] suggested an incentive mechanism for detecting selfish nodes in opportunistic networks. The aim of this approach was to diminish the issues of having selfish nodes in an opportunistic network.

Sahu and Sinha [19] suggested a cooperative approach for understanding the behavior of IDS in MANETs. In this paper, they described about various attacks and techniques used for intrusion detection which were proposed to provide high performance. Goyal and Singh [20] recommended an improved inverted table approach to detect selfish nodes in MANET. In this paper, a multi-dimensional trust management architecture was proposed to evaluate the trustworthiness of nodes in MANETs. Patel et al. [21] used an AODV protocol for trust-based routing in *ad hoc* networks. *Ad hoc* networks have limited physical security, less infrastructure, restricted power supply, mobility network, and changing network topology. Bao et al. [22] proposed a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs). In this paper, they analyzed and evaluated the existing trust management schemes in MANETs. Cho et al. [23] developed and analyzed a trust management protocol for mission group communication systems in MANET. The goal of this study was to identify optimal design settings through the evaluation of mathematical models developed using a quantitative modeling technique. Velloso et al. suggested a human-based model, which built a relationship between nodes in an *ad hoc* network [24]. They present a flexible trust model in *ad hoc* networks based on the concept of human trust.

In this paper, the proposed record- and trust-based selfish node detection in MANET was compared with existing systems such as 2ack scheme, credit-based system, reputation-based system, or acknowledgement-based system. Boopathi et al. [25] suggested a random 2ack scheme to detect the selfish nodes in MANETs. The 2ack scheme was a network layer technique to detect selfishness and to mitigate their effects. Due to the dynamic change in topology, finding the route was very difficult, which was the drawback of this paper. Demestiches et al. [26] identified and addressed the main problem of service configuration and distribution in a composite radio environment (SCD-CRE). Atlasis et al.

[27] suggested a learning automation (LA) method with equivalent bandwidth approximations in order to diminish the percentage of overestimation. In this paper, a preventive congestion control mechanism and a call admission control (CAC) problem were examined.

The existing approaches, tries to give a motivation for participating in the network function. The major weakness of those techniques was the demand for trusted hardware to secure the currency. In order to overcome these drawbacks, a RTBD method is proposed in this paper.

3 Proposed method

The main intent of this analysis is to handle and detect selfish nodes in MANET using the RTBD technique. In this paper, the trustworthiness of a node is evaluated based on their behavior. The basic idea is to build a trust model that provides a mechanism to evaluate the trust of its neighbors. The proposed trust scheme contains a powerful tool for the detection of unexpected node behaviors. Once the selfish nodes are detected, their neighbors can use this information to avoid cooperating with them, either for data forwarding, data aggregation, or any other cooperative function. Figure 2 shows the overall proposed system of the RTBD technique.

3.1 Route discovery

Route discovery allows any node in a MANET to dynamically discover a route to any node in MANET. The initial step of route discovery is to create the number of nodes with the indicated position. By sending the RREQ packet, the route is discovered between the source node and the destination node. A node initiating a route discovery broadcasts a RREQ message, which may be received by those nodes within wireless transmission range. If the route discovery is successful, the initiating node receives a route reply message listing a sequence of network hops.

3.2 Selfish node detection

The MANET is modeled and the nodes in the network are deployed according to the architectural model. Numerous nodes will be participating in the MANET for forwarding and transmitting the data packets between the source and destination. All the nodes in MANET perform the routing function as mandatory and they must forward traffic, which other nodes sent to it. Among all the nodes, some of the nodes will behave selfishly; these types of nodes are called selfish nodes. Any node in MANET may act selfishly, which means using its limited resources only for its own profit, since each node in a network has the resource constraints such as storage and battery limitations. This type of nodes likes to enjoy the profits provided by the resources of other nodes in the network. But it should not make its own resource accessible to others. These nodes intent to get the greatest benefits from the network while trying to preserve their own resources. The behaviors of the selfish nodes are shown below:

- *Do not forward RREQ messages.* This type of nodes does not forward the RREQ messages in MANET. It drops these packets to avoid being the route member for others.
- *Do not forward data messages.* This kind of selfish nodes will forward the messages, but it will not relay data messages and drop them. This misbehavior will impact the performance of MANET.
- *Delayed forwarding RREQ messages.* This kind of selfish nodes forwards the messages with a delay near the upper limit of timeout.
- *Do not forward RREP messages.* If this kind of selfish node exists in MANET, it will drop all RREP messages received by these nodes.

Existing explorations on selfish behaviors in a MANET mainly concentrates on network concerns. The main objective of this analysis is to enhance the performance of

Algorithm 1 Processing of RREQ and RREP messages

Begin
Initiate route discovery through authentic neighbors (); //*RREQ initialization by the source node*
Processes RREQ (); //*RREQ processing at intermediate node*
Propagates RREQ (); through its authentic neighbors
Generates and unicasts RREP ();
Switches to monitoring and identification Routine (); //*RREQ processing at target node*
Modifies and unicasts RREP (); //*RREP processing at intermediate node*
Processes RREP (); //*RREP processing at source node*
End

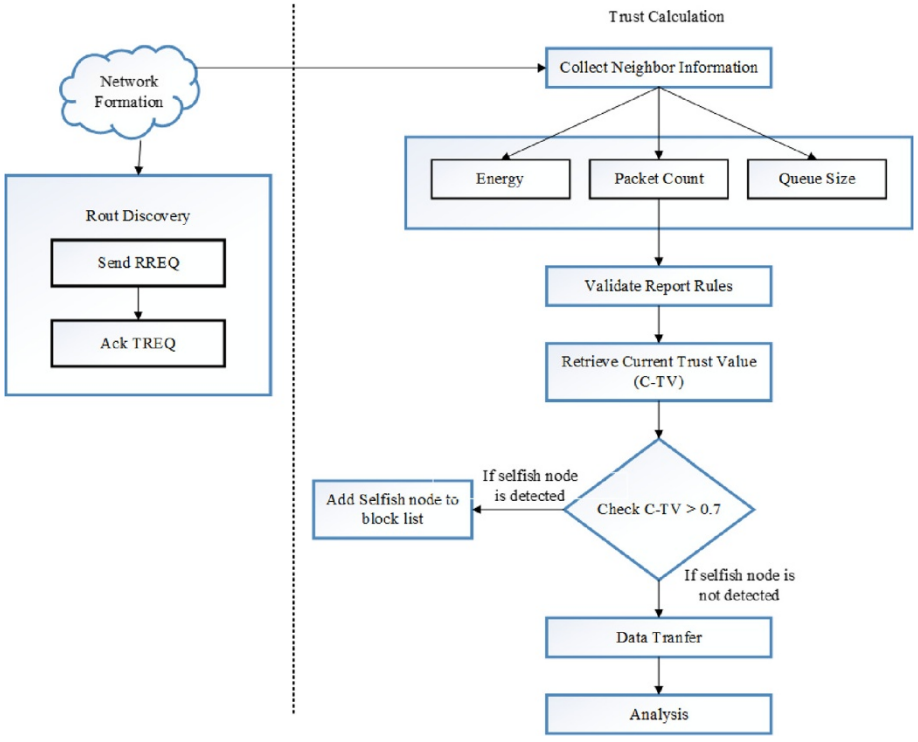

Figure 2 Overall flow of the proposed Record- and Trust-Based Detection (RTBD) technique.

MANET by detecting these types of selfish nodes using RTBD technique. In this paper, the problem of selfishness is addressed by using record-based trust mechanism.

3.3 Record- and Trust-Based Detection technique

In this framework, every node maintains a global trust state for all selfishly behaving nodes in the network. The trust state is maintained in the form of a trust table. A trust table contains two fields, namely *n-id* (*node id*) and *t-val* (*trust value*). When a node receives a new trust certificate, the trust state of a node is updated. The certificate is evaluated by verifying the response from every neighbour in the group. The impact of trust certificate in the final trust value of a suspected node depends on the trust state of the node. For updating the trust value of a node, the following function is used as shown in (1):

$$(1-T_{\text{new}}) = a(1-T_{old}) + b(1-T_c)-F \tag{1}$$

where a and b represent the weightage corresponding to the old trust and new trust values of the node. F is the trust replenishment factor over time. B depends on three factors a_1, a_2, and a_3. The parameter b can be expressed in (2):

$$b = a_1 \times a_2 \times a_3 \tag{2}$$

The parameter a_1 is shown in (3):

$$a_1 = \frac{\sum_{\text{maj}} W_i T_i}{W_n} \tag{3}$$

where W_i and T_i depicts the weightage and trust value, respectively, belonging to the majority group of the neighbors of the accused node. W_n is a factor that depends on the size of the network. a_2 represents the weightage given to the new trust value, and the value of a_3 is obtained using (4):

$$a_3 = \begin{cases} 1 \text{ if } k = 1 \\ 1 \text{ if } k > 1 \end{cases} \tag{4}$$

In this paper, the number of packets sent to the misbehaving nodes is reduced to mitigate the routing misbehavior. The following table shows the algorithm for detecting selfish nodes in MANET using RTBD technique.

Algorithm 2 Record- and Trust-Based Detection

//Route Discovery

Step 1: Source (S) sends a RREQ to destination (D).

Step 2: Destination (D) receives the RREQ from source (S) and sends RRES to source (S).

//Trust Calculation

Step 3: Neighbor information is gathered and sensed,

i. Energy.
ii. Packet Count.
iii. Queue Size.

Step 4: It generates a report and validate the report rules.

Step 5: The trust value is calculated using (5),

$$T_c^{ij} = \frac{t_s + p/2}{t + p} \qquad t_s,\ t \geq 0, p > 0 \tag{5}$$

where T_c is the trust calculation, ij represents the node i to j, D represents direct trust, t_s illustrates the time success, t is the time transactions, and p is the positive real number.

Step 6: The current trust value (C_TV) is retrieved.

```
if (C_TV > 0.7)
{
  if (selfish node is detected)
  Add selfish node to block list (B_L);
else
Transfer the data to destination node;
}
```

Step 7: Finally, the performance is evaluated.

The network congestion leads to reduction in throughput due to high load. The selfish node is verified for the data packet drop. Then, the selfish node is checked for false reporting; when the node misreports the data, it is block listed. These processes repeat for all the mobile nodes in MANET, thus obtaining the set of selfish nodes from the selfish nodes in the network. The packet transmission and the block list will decide whether the packet is available or not. All the aforementioned processes are repeated for the transfer of all packets. The packets are transmitted one by one at each iteration step until there is no packet available for further transmission. Each trust node receives the trust reports for each data packet transfer. The records are signed for further authentication and protection. These processes will enable the detection of the selfish nodes in the MANET (Table 1).

Q_{rs} is defined as the query request success rate, which is calculated based on the number of neighboring nodes who have successfully received RREQ from the source. Q_{rf} is defined as the query request failure rate, which is calculated based on the number of neighboring nodes who have not received RREQ. Q_{ps} represents the query reply success rate, which is calculated based on the successful replies received by the source. Q_{pf} describes the query reply failure, which is calculated based on the number of neighboring nodes, who have not sent the replies. Q_{ds} defined as the data success rate, which is calculated based on successfully transmitted data. Q_{df} determines the data failure rate based on the data, which have failed to reach the destination.

$$Q_{req} = \frac{Q_{rs} - Q_{rf}}{Q_{rs} + Q_{rf}} \tag{6}$$

Table 1 Trust value calculation parameters

Type	RREQ	RREP	Data
Success	Q_{rs}	Q_{ps}	Q_{ds}
Failure	Q_{rf}	Q_{pf}	Q_{df}

Table 2 Simulation setup parameters

Simulation parameter	Value
Simulator	NS-2 (v.2.34)
Simulation area	100 × 100 m
Number of nodes (x)	40
Transmitter range	250 m
Bandwidth	2.4 GHz
Packet size	512 bytes
Buffer length (MS_a)	50 bytes
Traffic type	Constant bit rate (CBR)
Simulation time	50 s
Receiver energy (R_x)	28.1838 mJ
Transmitter energy (T_x)	28.1838 mJ
Initial energy (E_i)	500 mJ

$$Q_{\text{res}} = \frac{Q_{\text{ps}} - Q_{\text{pf}}}{Q_{\text{ps}} + Q_{\text{pf}}} \tag{7}$$

$$Q_{\text{data}} = \frac{Q_{\text{ds}} - Q_{\text{df}}}{Q_{\text{ds}} + Q_{\text{df}}} \tag{8}$$

where Q_{req}, Q_{res}, and Q_{data} are intermediate values, which are used to calculate the node" request rate, response rate, and data transmission rate, respectively.

$$\text{TV} = T(\text{RREQ}) \times Q_{\text{req}} + T(\text{RREP}) \times Q_{\text{res}} + T(\text{DATA}) \times Q_{\text{data}} \tag{9}$$

where TV represents the trust level value and T(RREQ), T(RRES), and T(DATA) are time factorial for route request, route response, and data sent by the node, respectively.

4 Performance analysis

This section presents the results of the proposed method, namely RTBD technique. The proposed method has been implemented in the Network Simulator (NS2) version 2.34, and the performance of the proposed RTBD technique is compared with the existing selfish node detection, namely self-centered friendship (SCF) tree. Table 2 shows the simulation setup parameters and its values.

4.1 Identification of verified block listed nodes

The initial step involves the detection of the verified block listed nodes among the mobile nodes in MANET. The difference between the normal nodes and the verified block listed nodes is shown in Figure 3. The blue-colored nodes are the normal nodes, while the yellow-colored nodes indicate the verified block listed nodes.

4.2 Detection of selfish nodes

The selfish nodes among the verified block listed nodes are detected in the second step. The detected selfish nodes are highlighted in red color, which is shown in Figure 4.

4.3 Packet delivery ratio

Packet delivery ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and

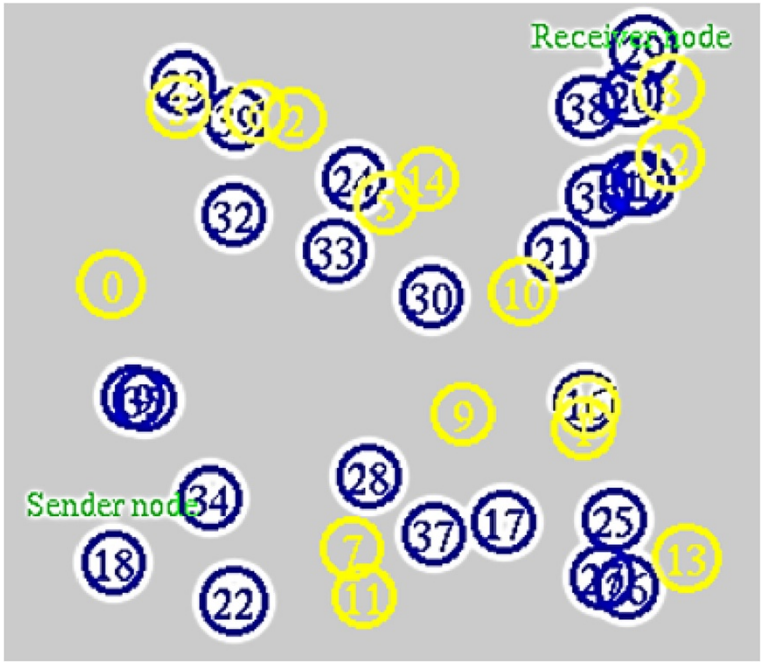

Figure 3 Difference between the normal nodes and the verified block listed nodes.

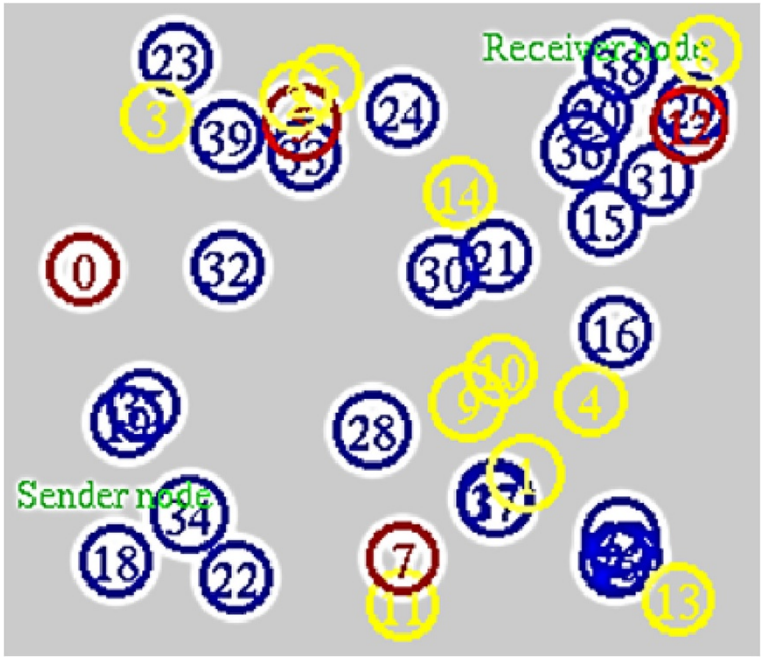

Figure 4 MANET along with selfish detected nodes.

the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols, and it characterizes both the correctness and efficiency of *ad hoc* routing protocols. Figure 5 shows the comparison graph between the existing SCF tree and the proposed RTBD technique. In this graph, the *x*-axis represents the number of nodes and the *y*-axis represents the packet delivery ratio in terms of percentage.

4.4 Average packet dropping

The implication of not forwarding the packets or dropping the packets in MANET leads to a serious problem. So, this analysis addresses this event and gives higher priority for packet dropping in MANET. The packet drop rate is observed in the selfish node detection methods, namely SCF and RTBD. The comparative analysis with respect to the number of nodes is shown in Figure 6. In this graph, the *x*-axis represents the number of selfish nodes and the *y*-axis represents the average for dropping packets.

4.5 Detection rate

Selfish node detection is an important concern in MANET, so this study fully concentrates the detection of selfish nodes in an efficient manner by using RTBD

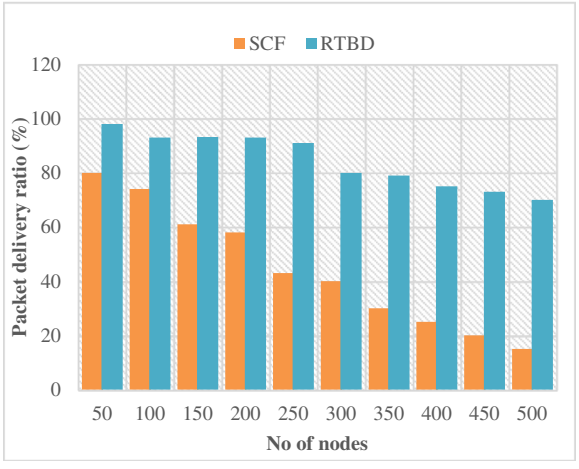

Figure 5 Packet delivery ratio.

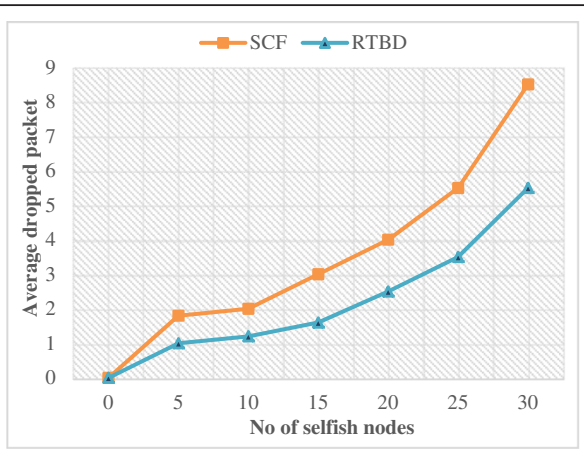

Figure 6 Average packet dropping.

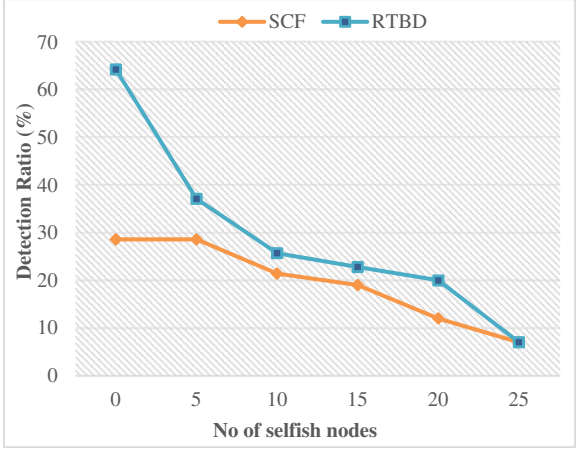

Figure 7 Detection ratio.

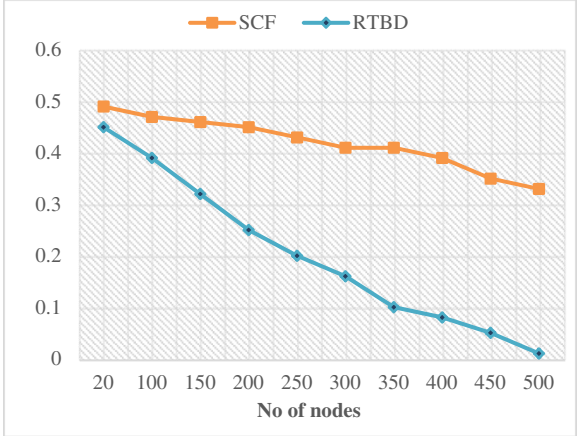

Figure 9 Average latency.

technique. The detection rate of the selfish behavior is observed by using the RTBD method. Compared to the SCF method, the proposed RTBD method significantly increases the detection ratio. The comparative analysis between the existing SCF and the proposed RTBD method is shown in Figure 7. In this graph, the *x*-axis represents the number of selfish nodes and the *y*-axis represents the detection ratio in terms of percentage.

4.6 False positive rate

The false alarm will be differentiated from the overall selfishness alarm. The detection of this false alarm leads to better performance in the overall network. The probability of parameters such as energy, memory space, and CPU time in packet drop rates is analyzed with respect to the false alarm rate. The comparison between the existing SCF and the proposed RTBD technique is shown in Figure 8. In this graph, the *x*-axis represents the number of selfish nodes and the *y*-axis represents the false positive rate in terms of percentage.

4.7 Average latency

Latency is comparable to twice the query time, since the sender node sends a request and receives an acknowledgement and then starts transfer from the first answering node. In this analysis, the latency and the control overhead are reduced by using RTBD-based selfish node detection method. Compared to the existing SCF method, RTBD has significantly lower overhead and latency. Latency is defined as the average time taken by the packet to reach the destination node from the sender node. It differs depending on the location of specific pairs of communicating nodes. Figure 9 shows the comparative analysis between the proposed RTBD technique and the existing SFC technique. In this graph, the *x*-axis represents the number of nodes and the *y*-axis represents the average latency.

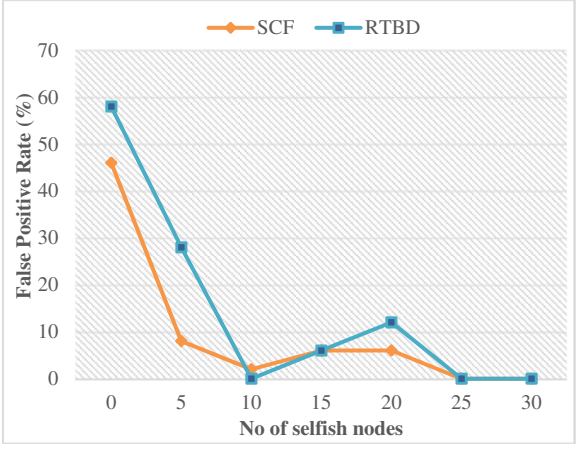

Figure 8 False positive rate.

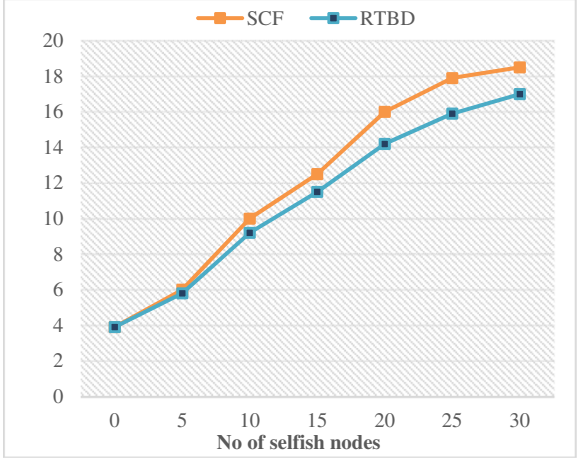

Figure 10 Average overhead.

4.8 Average overhead

Figure 10 shows the routing overhead with respect to the number of selfish nodes. Moreover, heavier load results in more packet drops in MANET. In this analysis, the proposed RTBD technique incurs less overhead than the existing SCF method. In this graph, the *x*-axis represents the number of selfish nodes and the *y*-axis represents the average overhead.

5 Conclusions

The misbehavior of selfish nodes is a major problem in MANET. The selfish nodes do not participate in the routing process, which intentionally delay and drop the packet. These misbehaviors of the selfish nodes will impact the efficiency, reliability, and fairness. The selfish node utilizes the resources for its own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the selfish nodes in MANET. This study proposes a new technique, namely RTBD, to detect the selfish nodes in an efficient manner. The suggested RTBD method is an effective method, which enhances the performance of MANET. It significantly improves the performance metrics such as PDR and detection ratio. Moreover, it diminishes the overhead, latency, and packet dropping ratio. Compared to the existing SCF method, the proposed method competently detects the selfish nodes in MANET.

The future enhancement can be done by providing the security to the neighbor node. This avoids the neighbor node being compromised by the selfish node.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Department of Computer Science and Engineering, University College of Engineering Pattukottai, Tamil Nadu 614701, India. [2]Department of Information Technology, M.A.M College of Engineering, Thiruchirappalli, India. [3]Department of Computer Science and Engineering, S.A. Engineering College, Chennai, India.

Received: 10 July 2014 Accepted: 29 October 2014
Published: 29 November 2014

References

1. C Jae-Ho, S Kyu-Sun, L SangKeun, W Kun-Lung, Handling selfishness in replica allocation over a mobile ad hoc network. IEEE Transactions on Mobile Computing **11**, 278–291 (2012)
2. BG Ryu, JH Choi, S Lee, Impact of node distance on selfish replica allocation in a mobile ad-hoc network. Ad Hoc Netw. **11**, 2187–2202 (2013)
3. H Sedghi, MR Pakravan, MR Aref, A misbehavior-tolerant multipath routing protocol for wireless ad hoc networks. Int J Res Wireless Syst **2**(2), 6–15 (2013)
4. M Mejia, N Peña, JL Muñoz, O Esparza, MA Alzate, A game theoretic trust model for on-line distributed evolution of cooperation in MANETs. J. Netw. Comput. Appl. **34**, 39–51 (2011)
5. R Singh, P Singh, M Duhan, An effective implementation of security based algorithmic approach in mobile adhoc networks. Hum Centric Comput Inf Sci **4**, 1–14 (2014). 06/19 2014
6. E Hernández-Orallo, MS Olmos, J-C Cano, C Calafate, P Manzoni, A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. Wirel. Pers. Commun. **74**, 1099–1116 (2014). 02/01 2014
7. V Manoj, N Raghavendiran, M Aaqib, R Vijayan, Trust based certificate authority for detection of malicious nodes in MANET, in *Global Trends in Computing and Communication Systems. vol. 269*, ed. by PV Krishna (Springer, Berlin, 2012), pp. 392–401
8. I Jawhar, Z Trabelsi, J Al-Jaroodi, Towards more reliable and secure source routing in mobile ad hoc and sensor networks. Telecommun. Syst. **55**, 81–91 (2014)
9. A Rodriguez-Mayol, J Gozalvez, Reputation based selfishness prevention techniques for mobile ad-hoc networks. Telecommun. Syst. 1–15 (2013)
10. F Afghah, A Razi, A Abedi, Stochastic game theoretical model for packet forwarding in relay networks. Telecommun. Syst. **52**, 1877–1893 (2013)
11. E Hernandez-Orallo, MD Serrat, JC Cano, CT Calafate, P Manzoni, Improving selfish node detection in MANETs using a collaborative watchdog. Commun Letters IEEE **16**, 642–645 (2012)
12. S Padiya, R Pandit, S Patel, Survey of innovated techniques to detect selfish nodes in MANET. IJCNWMC **3**(1), 221–230 (2013)
13. DB Roy, R Chaki, MADSN: mobile agent based detection of selfish node in MANET. Int J Wireless Mobile Networks (IJWMN) **3**(4), 225–235 (2011)
14. D Koshti, S Kamoji, Comparative study of techniques used for detection of selfish nodes in mobile ad hoc networks. Int J Soft Comput Eng (IJSCE) **1**(4), 190–194 (2011)
15. R Patil, S Kallimath, Cross layer approach for selfish node detection in MANET. Int J Adv Res Electronics Commun Eng **1**, 77–81 (2012)
16. A Kurkure, B Chaudhari, Selfish node detection techniques in MANET: a review. Int J Comput Sci Manage Res, 88–94 (2013)
17. N Nandhini, S Ramesh, PG Kumar, Effective ant based routing algorithm for data replication in manets. ICTACT J Commun Technol **4**, (2013)
18. R-I Ciobanu, C Dobre, M Dascalu, S Trausan-Matu, V Cristea, Collaborative selfish node detection with an incentive mechanism for opportunistic networks, in *International Symposium on Integrated Network Management (IM 2013), 2013 IFIP/IEEE* (Ghent, 2013), pp. 1161–1166
19. L Sahu, C Sinha, A cooperative approach for understanding behavior of intrusion detection system in mobile ad hoc networks. Int. J. Comput. Sci. **1**(1), 24–30 (2013)
20. S Goyal, I Singh, An improved inverted table approach to detect selfish node in mobile ad hoc network. Int. J. Appl. Eng. Res. **7**, (2012)
21. DG Patel, PA Pandey, MC Patel, Trust based routing in ad-hoc networks. Int J Curr Eng Technol **4**(2), 860–863 (2014)
22. F Bao, R Chen, M Chang, JH Cho, Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. Network Serv Manage IEEE Trans **9**, 169–183 (2012)
23. J-H Cho, A Swami, I-R Chen, Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. J. Netw. Comput. Appl. **35**, 1001–1012 (2012)
24. PB Velloso, RP Laufer, D d O Cunha, Trust management in mobile ad hoc networks using a scalable maturity-based model. Network Serv Manage IEEE Trans **7**, 172–185 (2010)
25. GM Boopathi, N Insozhan, S Vinod, Selfish nodes detection using random 2ack in MANET's. IJESE **1**(4), 3–5 (2013)
26. PP Demestichas, V-AG Stavroulaki, L Papadopoulou, AV Vasilakos, ME Theologou, Service configuration and traffic distribution in composite radio environments. IEEE Trans Syst Man Cybern B Cybern **34**, 69–81 (2004)
27. AF Atlasis, NH Loukas, AV Vasilakos, The use of learning algorithms in ATM networks call admission control problem: a methodology. Comput. Netw. **34**, 341–353 (2000)

doi:10.1186/1687-1499-2014-205
Cite this article as: Subramaniyan *et al.*: **A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique.** *EURASIP Journal on Wireless Communications and Networking* 2014 **2014**:205.