Journal of King Saud University – Computer and Information Sciences (2016) **28**, 289–302

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Erlang coefficient based conditional probabilistic model for reliable data dissemination in MANETs

R. Manoharan, J. Sengathir *

Department of Computer Science and Engineering, Pondicherry Engineering College, ECR, Pillaichavady, Pondicherry 605014, India

Received 30 January 2014; revised 25 June 2014; accepted 23 October 2014
Available online 2 November 2015

KEYWORDS

Selfish nodes;
Reputation;
Genuineness factor;
Conditional Probabilistic Coefficient;
Erlang coefficient;
Network resilience

Abstract In MANETs, reputation plays a significant role in reliable dissemination of data for establishing maximum degree of cooperation among the mobile nodes in the network. But, the presence of selfish nodes drastically reduces the level of cooperation between the nodes and further reduces the life time of the network. Moreover, when the number of selfish nodes increases in the network, the packet delivery ratio and throughput decreases which in turn increases the number of retransmissions. Hence, an effective mechanism for isolating selfish nodes in order to increase the packet delivery rate and the throughput for reliable dissemination of data becomes vital. This paper proposes an Erlang coefficient based conditional probabilistic model (ECCPM) which makes the decision of isolating selfish nodes through the manipulation of Conditional Probabilistic Coefficient (CPC) factor. This Conditional Probabilistic Coefficient acts as the reputation factor for estimating the level of negative impact produced by selfish nodes toward the resilience of the network. The proposed work is simulated in ns-2 and from the results, it is obvious that ECCPM showed better performance in terms of packet delivery ratio, throughput, control overhead and total overhead than existing mitigation mechanisms like RCSBMM, RFBMM, SHRCM and PCMA proposed for selfish nodes.

1. Introduction

From the recent past, wide range of techniques were proposed for enabling reliable transmission of data in multi-hop ad hoc networks. Since, the nodes in mobile ad hoc networks do not possess a centralized infrastructure they rely on the reputation of the intermediate nodes as routers for forwarding packets between the source and destination (Buttyan and Hubaux, 2003; Khaled Ahmed Abood Omer, 2009). This reputation depends on the extent of cooperation rendered by each and every mobile node present in the ad hoc environment (Yaser Khamayseh et al., 2011), (Senthilkumaran and Sankaranarayanan, 2013). But, there exists a class of nodes called selfish nodes in MANETs which does not forward packets from neighbor nodes in order to conserve its resources (Buchegger and Boudec, 2002a). Hence, the presence of selfish

* Corresponding author. Tel.: +91 9486013072.
E-mail addresses: rmanoharan@pec.edu (R. Manoharan), j.sengathir@gmail.com (J. Sengathir).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.10.008
1319-1578 © 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

node reduces the cooperation level and affects the reliable dissemination of data.

Reputation based approaches plays a significant role in detecting and isolating selfish nodes. In a reputation system, the reliability of a mobile node was identified based on the reputation value, that reflects the behavior of nodes (Marti et al., 2000; Gamal Abdel Fadeel Mohamed Khalaf and Hesham Zarief Badr, 2013). In general, reputation based approaches were categorized into first hand and second hand reputation approaches. In which, first hand reputation approach relies on information obtained through direct interaction with the mobile nodes while second hand reputation approach depends on the information obtained from neighbor nodes.

Most of the proposed reputation based mechanisms contributing to mitigating selfish nodes have not taken conditional probability into account. Conditional probability can be used to model events for detecting selfishness based on present and past behavior of the mobile nodes. Hence conditional probabilistic based reputation mechanisms may effectively mitigate selfish nodes in an efficient manner.

The proposed ECCPM uses an Erlang coefficient computed based on conditional probability which analyses the reputation of mobile nodes and resilience of the entire network with aid of Conditional Probability Coefficient factor. In this approach, we consider a MANET environment where each node has a unique identity and monitors their neighbors for identifying selfishness. To detect selfish nodes, the following two factors are considered: First, the genuineness of the each node based on the packet drop when the energy level of the mobile node reaches below the minimal residual energy. Secondly, impact of the nodes reputation on the resilience of the routing path.

This paper is intended to answer the following questions that are related to

(a) The impact of selfish nodes toward the resilience of the network.
(b) The role of Erlang distribution in quantifying the reputation of the mobile nodes.
(c) The effectiveness of ECCPM in identifying selfish nodes when compared to the existing works of the literature.
(d) The efficiency of ECCPM in framing maximum and minimum threshold range for detecting selfish nodes.

The remaining part of the paper is organized as follows: Section 2 presents a brief description of some of the reputation based approaches proposed for detecting and isolating selfish nodes. Section 3 elaborates on the Erlang coefficient based conditional probabilistic model (ECCPM) and its supports toward detection and isolation of selfish nodes present in the network. An exhaustive simulation study conducted for evaluating the performance of ECCPM model is presented in section 4. Section 5 concludes the paper.

2. Related work

A vast number of reputation based mitigation mechanisms proposed for selfish nodes were contributed in the recent past and are thoroughly analyzed and detailed below.

A competent reputation framework was proposed by Marti et al. (2000) for identifying misbehaving nodes based on the two levels of rating namely suspected rating and neutral rating. These rating levels were estimated based on watchdog and path rater mechanisms. The core idea behind this reputation framework was to isolate the non-cooperating malicious nodes from the routing activity than punishing them. Another Bayesian theorem based reputation mechanism is proposed by Buchegger and Boudec (2002b), which estimates the level of reputations attributed by each and every node toward the efficient routing of packets in the network. They considered both uniform and beta distribution for modeling events that helps in identifying malicious nodes. Wang and Li (2006) contributed a cooperative enforcement mechanism which incorporates strategy proof pricing approach. This centralized algorithm further incorporates an optimal time complexity for computing payment based on least cost path. Paul and Westhoff (2002) proposed a distributed mechanism for dealing with selfish behavior of nodes in an ad hoc environment. This context-aware mechanism identifies malicious behavior of nodes that could result in non-repudiation responses.

Further, Kargl et al. (2004) contributed a trust based evidence framework with the help of routing protocol named as SDSR. SDSR optimally performs the routing decision based on the method of negotiation. The capacity of over healing is the important characteristic feature of this approach. They proposed security architecture called SAM for mitigating selfish nodes in an efficient manner. Chen and Varatharajan (2009) proposed a Dempster Shafer theory based selfish node detection framework for estimating the degree of cooperation rendered by mobile nodes using posterior probability. They also used a numerical procedure for combining multiple evidences into single value of evidence gathered through second hand reputation mechanism. Yanwei Wu et al. (2010) proposed an efficient routing scheme based on Nash equilibrium which maximizes nodes' profit by enforcing cooperation. This detection mechanism analyses both the link layer reliability and transport layer reliability. This detection mechanism further avoids hidden actions and hidden information which could lead to imperfect monitoring. Laoutaris et al. (2007) contributed a caching algorithm that deals with cache state interactions and common adoption policies. This caching approach aids in categorizing mobile nodes into rational, self-aware and selfish nodes through content networking applications.

Furthermore, Michiardi and Molva (2002) contributed a watch dog based collaborative scheme for detecting malicious nodes. They categorized reputation levels for detecting selfish nodes into three types' viz., functional reputation, subjective reputation and indirect reputation. This mechanism isolates selfish nodes based on information obtained from neighbors. They developed a mechanism that isolates selfish nodes based on the threshold level of packet dropped by them. Rizvi and Elleithy (2009) proposed a time division based scheme for isolating malicious behavior of nodes. They clarified the misconceptions that created ambiguity about selfishness and misbehavior of nodes. They proposed consistent trust and cooperation mechanism for enhancing resource sharing. In addition, they analyzed the performance of the ad hoc network through critical network parameters like network utilization and transmission overhead. Bo Wang et al. (2005) proposed a reputation mechanism that detects and punishes selfish nodes based on local detection strategy. This local assessment algorithm aids in classifying the mobile nodes into cooperative and selfish nodes with the aid of self-statistical tests performed based on finite state model. Komali et al. (2008) proposed a selfish mitigation mechanism that effectively deals with energy consumption and network connectivity. This mitigation mechanism integrates two algorithms viz., Max-Improvement algorithm and δ – Improvement algorithm. In this mechanism, the mobile node was identified as selfish based on the analysis carried out through the Nash properties developed for effective topology design.

In addition to this, a reliability framework for identifying malicious behavior of nodes were proposed by Zouridaki et al. (2009)) which is based on reputation level computed through first and second hand information gathered from neighbor nodes. They used opinion metric as a unique factor for identifying malicious nodes. They made a statistical prediction about the reliability of data packets delivered through trust and confidence limits. Watch dog based reputation framework was contributed by Hernandez-Orallo et al. (2012). In this, the presence of selfish nodes was identified based on two parameters viz., total overhead and detection time computed through transition probability matrix. They also used NO INFO and POSITIVE as two continuous time Markov states for categorizing possible behavior of mobile nodes. Eidenbenz et al. (2008) contributed a COMMIT protocol for dealing with selfish nodes in order to prevent the exploitation of network utility. This COMMIT protocol integrates game-theoretic technique with VCG payment scheme for punishing misbehaving nodes. Sintanyehu Dehnie and Stefano Tomasin (2010) innovated a cooperative MAC protocol uniformly more powerful test and probability ratio test. This cooperative mechanism analyses the effect of fading and interference that could originate by the presence of selfish or malicious nodes.

Yet, Hongxun Liu et al. (2007) proposed a two-timer scheme that detects selfish nodes by categorizing packets into control packets and data packets. These classifications of packets were achieved by means of a drop counter, which gets updated whenever a packet enters or leaves a node. The mobile node was identified as malicious when the drop counter exceeds the threshold value. Annapourna et al. (2011)) proposed an energy efficient algorithm that integrates two metrics viz., transmission power and remaining energy capacity into the AODV protocol which in turn increases the life time of the mobile node. This energy based routing algorithm chooses between maximum remaining energy capacity route and minimum transmission route for enabling efficient routing. Binglai Niu et al. (2011) proposed a cooperation stimulation mechanism based on tit for tat strategy for punishing malicious behavior of nodes. They also contributed a novel interval based assessment approach to address the issue of imperfect monitoring in the presence of misbehaving nodes.

Finally, the four bench mark selfish node mitigation mechanisms compared with ECCPM are discussed below.

Fahad and Askwith, 2006) proposed a Packet Conservation based Monitoring Algorithm (PCMA) which detects selfish nodes with the help of dual information obtained from the neighbors of the mobile nodes. This mechanism mainly targets on the detection of a special kind of selfish node that intentionally drops packets in a partial manner. Further, this PCMA algorithm did not rely on the information obtained from suspicious node. This mechanism also assumes that, all the mobile nodes in the topology move in a collision free environment. In addition, they possess the capacity to classify packets that were dropped due to error and congestion. Sengathir and Manoharan (2013a) proposed a Reliability Factor based Mathematical Model (RFBMM) to isolate the selfish nodes based on the reliability factor computed for each and every node using second hand reputation technique. This mechanism, initially computes the normalized deficiency factor through the primary and secondary normalized deficiency factor based on packet delivery rate. This mechanism, further manipulates the packet deficiency factor through the sum of product of normalized deficiency factor and their associated weights. Furthermore, this mechanism estimates the reliability of the mobile node through exponential distribution. Finally, the node was confirmed as selfish, when the reliability factor was found to be less than 0.3 and it was isolated from the network.

Sengathir and Manoharan (2014) also contributed a Split half Reliability Coefficient based Mathematical Model (SHRCM) for mitigating selfish nodes based on split half reliability co-efficient computed in two steps viz., through the computation of Karl Pearson correlation coefficient and revaluation done through spearman brown formula. This mechanism, initially determines the cumulative sum of packets entering or leaving a mobile node through which sum of squares of deviation of the incoming and outgoing packets of mobile nodes were manipulated. Then, Karl Pearson correlation coefficient was applied to estimate the reputation of mobile nodes through the sum of squares of deviation. Further, this mechanism confirms a node as selfish when the value of correlation coefficient was found to be less than zero. Furthermore, this mechanism reconfirms a node as selfish by reevaluating through a correlated reliability coefficient factor which was estimated through Spearman Brown Formula. Finally, the node was confirmed as selfish and isolated from the network, when the correlated reliability coefficient value was found to be less than 40 percent. In addition to this, Sengathir and Manoharan (2013b) proposed a Reliable Conditional Survivability based Mathematical Model (RCSBMM) that manipulates the survivability coefficient of the network based on Laplace stleltjes transform. This RCSBMM also determines two parameters viz., failure rate of selfish nodes and failure rate of cooperative nodes based on theorem of total transform. This mechanism further, confirms a mobile node as selfish when its reliable conditional survivability coefficient was less than 0.30. This mechanism also aids in framing a threshold value to network survivability.

2.1. Extract of the literature

The reputation based approaches for detecting and isolating selfish nodes available in the literature has the following pitfalls:

(a) A conditional probabilistic based reputation mechanism using Erlang distribution (which predicts the behavior of an entity based on the events modeled through two continuous time distributions viz., exponential and gamma distribution) for mitigating selfish node behavior has not been investigated to the best of our knowledge.

(b) A mechanism that efficiently enhances reliable dissemination of database considering the reputation of individual nodes and the resilience of the entire network has not been explored.

(c) Hence, these pitfalls have motivated us for devising an innovative Erlang coefficient based reputation mechanism for mitigating selfish nodes

3. Erlang coefficient based conditional probabilistic model (ECCPM)

3.1. Problem statement

In ECCPM, we consider an ad hoc network in which each and every mobile node is having a unique identity. To achieve the goal of detecting and isolating selfish nodes the following key points have to be considered. First, the probability of packet delivery rate of each mobile must be quantified to analyze the genuineness factor of that node. Secondly, the non-cooperativity factor has to be estimated for determining the impact caused due to the increase in the number of selfish nodes in the network. Finally, the network resilience has to be measured to analyze the negative impact of selfish nodes toward reliability of the network.

This ECCPM is a conditional probability based mitigation mechanism proposed for detecting and isolating selfish nodes, in which the events are modeled with Erlang distribution. It isolates the selfish nodes from the routing path based on a factor called Conditional Probabilistic Coefficient (CPC). This coefficient computes the reputation level of each and every mobile node participating in the routing activity based on which selfish nodes are isolated. It also quantifies the impact of selfish nodes toward the resilience of the entire network.

Further, ECCPM is a distributed mechanism for detecting and isolating selfish nodes, in which the reputation is calculated in each and every mobile node rather than any centralized node. This distributed mechanism implemented in ECCPM certainly increases the overhead which is negligibly small and further, it is experimentally tested and detailed in section 4.

The ECCPM approach isolates selfish nodes through the following four steps.

a. Detection of Selfish node based on genuineness factor (G_F)
b. Estimation of Non-cooperativity factor (λ)
c. Determination of CPC based on Erlang distribution.
d. Decision on Isolation of Selfish nodes based on CPC.

3.2. Detection of selfish node based on genuineness Factor(G_F)

ECCPM detects the selfish nodes present in the routing path purely based on the value of genuineness factor (G_F). The Genuineness Factor (G_F) is computed for each and every mobile node by their neighbors as follows.

Let $NP_{r(1)}$, $NP_{r(2)}$, $NP_{r(3)} \ldots NP_{r(k)}$ and $NP_{f(1)}$, $NP_{f(2)}$, $NP_{f(3)} \ldots NP_{f(k)}$ be the number of packets received and forwarded by a mobile node as monitored by their neighbor in k sessions respectively.

The probability of packet delivery (PPD) for a mobile node in a session is given by Eq. (1)

$$\mathrm{PPD}_i = \frac{\mathrm{NP}_{f(i)}}{\mathrm{NP}_{r(i)}}, where 1 \leqslant i \leqslant k \tag{1}$$

The average value of PPD computed for the entire 'k' sessions is represented by Eq. (2)

$$\mathrm{APPD}_k = \frac{\sum_{i=1}^{k} \mathrm{PPD}_i}{k} \tag{2}$$

The Normalized Reputation Factor 'NRF' is computed based on the value of APPD for each and every mobile node by their neighbors and is represented in Eq. (3)

$$\mathrm{NRF} = \frac{2^{\mathrm{APPD}_k - \mathrm{NL} - \mathrm{NU}}}{\mathrm{NU} - \mathrm{NL}} \tag{3}$$

where, NU – upper bound value of normalization (+1), NL – lower bound value of normalization (−1). The genuineness factor (G_F) identified for a mobile node by their neighbors is given by Eq. (4)

$$G_F = e^{-\mathrm{NRF}} \tag{4}$$

Here the upper bound and the lower bound values of normalization are considered as +1 and −1. This is because, we require NRF to reflect the reliability of a node in terms of packet delivery. Hence, the values obtained for NRF may be either positive or negative.

The ECCPM approach decides a mobile node as selfish or cooperative based on the value of G_F. When the value G_F of a mobile node is found below 0.50 as proposed in (Amir Khusru Akhtar and Sahoo, 2008), the node is identified as selfish.

The following algorithm 1 illustrates the steps to estimate the Genuineness Factor (G_F) in each and every mobile node present in the routing path. Based on the value of G_F obtained for a mobile node, the behavior of a particular node is classified as either selfish or cooperative.

Algorithm 1: Estimation of Genuineness Factor (G_F).
Notations:

n-total number of Mobile Nodes in the routing path.
V_j-represents a node for which, G_F is computed where $1 \leqslant j \leqslant n$
P_f-number of packets forwarded by a mobile node to its neighbors.
P_r-number of packets received by a mobile node from its neighbors.
k-number of sessions.
NU-Upper bound normalized value (+1)
NL-Lower bound normalized value (−1)
Algorithm (Estimation of G_F)

```
Begin
For each and every mobile node $j = 1$ to $n$ do
For each and every session $l = 1tokdo$
Compute the probability of packet delivery of a node by $V_j[PPD(l)] = \frac{V_j[NP_f(l)]}{V_j[NP_r(l)]}$;
Summation of packet delivery rate of all the $k$ sessions is done by$s[l] = s[l] + V_j[PPD(l)]$;
End for
Compute average value of packet delivery rate of a node in k sessions using $A[j] = \frac{s[l]}{k}$;
```

```
 8. Calculate the normalized reputation factor using $V_i[NRF] = \frac{2^{A[j]-NU-NL}}{NU-NL}$;
 9. Calculate Genuineness Factor using $V_j[G_F] = e^{-V_j[NRF]}$;
10. If the genuine factor of a mobile node $V_j(G_F) < 0.5$ then
11. $V_j$ is a selfish node
12. Else
13. $V_j$ is a cooperative node
14. End If
11. End for
12. End
```

Fig. 1 illustrates an ad hoc environment, in which the routing path is considered as S → 6 → 1 → 4 → 3 → 5 → D, where S and D are designated as source and destination nodes respectively. Our ECCPM approach estimates the reputation level of mobile nodes present in the routing path through the value of G_F. In this scenario, the G_F values for the nodes 1 and 4 are found to be less than the threshold value (0.5). Hence, these nodes are identified as selfish.

3.3. Estimation of non-cooperativity factor (λ)

The non-cooperativity factor (λ) depends on the number of cooperative nodes and selfish nodes present in the routing path established between the source and the destination. Within a network life time x, if a set of nodes in the routing path is said to be selfish with the genuineness factor G_F then at the same time, the remaining nodes are said to be cooperative with the genuineness factor (1-G_F) represented by the Eqs. (5) and (6)

$$c_x(r = 0) = 1 - G_F \tag{5}$$

$$s_x(r = 1) = G_F \tag{6}$$

where 'r' is the random variable used for differentiating selfish nodes from cooperative nodes.

The number of cooperative nodes and selfish nodes in the network are designated as c and s respectively. The non-cooperativity factor is defined as the degree of non-cooperation rendered by each and every mobile node of the network. This non-cooperative factor determined in terms of packet delivery rate with specific genuineness factor is computed through Eq. (7) and its simplified expression given by (8)

$$\lambda = \frac{n}{c} * (1 - G_F) + \frac{n-c}{c} * G_F \tag{7}$$

$$\lambda = \frac{n - (c * G_F)}{c} \tag{8}$$

where 'n' is the total number of nodes present in the network. Since, the non-cooperativity factor depends on all the mobile nodes present in the network.

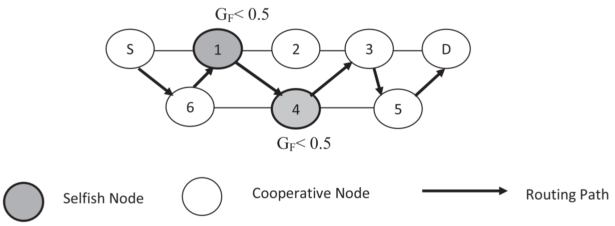


Figure 1 Identification of selfish nodes using G_F.

The following algorithm 2 illustrates the steps in estimating the non-cooperativity factor (λ) for the entire routing path based on the total number of selfish and cooperative nodes present in the environment.

Algorithm 2: Estimation of non-cooperativity (λ). Notations:

n-total number of Mobile Nodes in the routing path.
V_j-represents a node whose G_F to be computed where $1 \leqslant j \leqslant n$
G_F-genuineness factor
r-a random variable used to categorize selfish from cooperative.
c-cooperative nodes
s-selfish nodes

Algorithm (Estimation of λ)

```
 1. Begin
 2. For each and every mobile node j = 1 to n do
 3. If $V_j(G_F) < 0.5$ then
 4. Set the random variable (r) for nodes identified as selfish using $V_j(r) = 1$
 5. Else
 6. Set the random variable (r) for that node as $V_j(r) = 0$
 7. End If
 8. End for
 9. For each and every mobile node j = 1 to n do
10. If $(V_j(r) = 1)$ then
11. Count the number of selfish nodes using $s = s + 1$;
12. End If
13. Count the number of cooperative node using $c = n - s$;
14. Compute the Non - Cooperativity factor ($\lambda$) of a mobile node toward network resilience using

$\lambda = \frac{n - (c * V_j(G_F))}{c}$;

 1. End for
 2. End
```

Fig. 2(a) illustrates an ad hoc environment, in which the routing path is considered as S → 6 → 1 → 4 → 3 → 5 → D, where S and D are designated as source and destination nodes respectively. Here, node 1 is identified as selfish based on the value G_F. Hence, the number of selfish nodes (s) in the routing path is found to be 1 and remaining nodes are counted as cooperative nodes (c). Now, our ECCPM approach estimates the non-cooperative factor for the entire routing path using Eq. (8). In this scenario, the value of non-cooperativity is estimated as λ = 0.71.

Fig. 2(b) illustrates an ad hoc environment, in which the routing path is considered as S → 6 → 1 → 4 → 3 → 5 → D, where S and D are designated as source and destination nodes respectively. Here, node 1, 4 and 3 are identified as selfish based on the value G_F. Hence, the total number of selfish nodes (s) in the routing path is found to be 3 and remaining nodes are identified as cooperative nodes (c). Now, our ECCPM approach estimates the non – cooperative factor for the entire routing path using Eq. (8). In this scenario, the value of non-cooperativity is estimated as λ = 1.35.

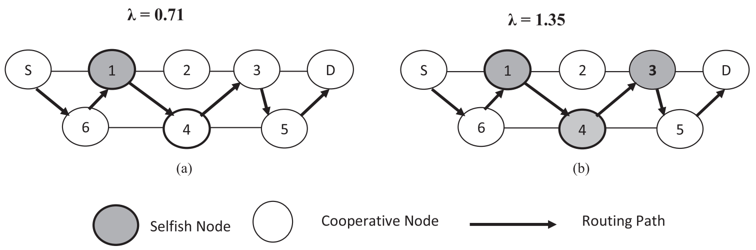


Figure 2 Estimation of non-cooperativity factor using ECCPM.

3.4. Determination of CPC based on Erlang distribution

The ECCPM approach calculates CPC based on the failure rate of cooperative nodes and failure rate of selfish nodes present in the routing path within the life time x. Thus, the failure rate of cooperative nodes with genuineness factor (1-G_F) is given by Eq. (9)

$$f_c = \lambda e^{-\lambda t} \tag{9}$$

In contrast, the failure rate of selfish nodes with genuineness G_F factor is Erlang distributed which is represented by the Eq. (10)

$$f_s = \lambda^2 t e^{-\lambda t} \tag{10}$$

Since, Erlang distribution is a special kind of phase type distribution, which highly depends on the sum of two independent exponential random variables. This distribution may be used to estimate the failure rate of the entire routing path. At the same time, the computation of failure rate of selfish nodes becomes vital because it further decreases the reputation level of the mobile nodes participating in the routing activity and furthermore, the failure of that mobile node may affect the resilience of the network.

Hence, the failure rate for the entire routing path can be calculated by using the Eq. (11)

$$f_{rp} = \lambda(1 - G_F)e^{-\lambda t} + \lambda^2 G_F t e^{-\lambda t} \tag{11}$$

Since, the failure rate of the entire network depends on either the failure rate of cooperative node or the failure rate of selfish node.

Thus, the Conditional Probabilistic Coefficient (CPC), calculated based on f_{rp} for identifying the impact of selfish nodes toward the resilience of the entire network is given by Eq. (12)

$$CPC = (1 + G_F \lambda t)e^{-\lambda t} \tag{12}$$

The following algorithm 3, illustrates the steps for estimating failure rate of the entire network based on CPC computed by considering the failure rate of selfish nodes and cooperative nodes present in the network.

Algorithm 3: Determination of CPC based on Erlang distribution. Notations:

n-total number of mobile nodes in the network.
λ–Non-cooperativeness factor
t-time instant.
r-a random variable represents the level of cooperation
f_s-Failure rate of the selfish node
f_c-failure rate of the cooperative node
f_N-failure rate of the entire network

```
Algorithm (Computation of CPC)
1. Begin
2. for the entire network do
3. Compute the failure rate of selfish nodes (s) using Erlang
   distribution based on, $f_s = \lambda^2 t e^{-\lambda t}$;
4. Compute the failure rate of cooperative nodes (c)using
   $f_s = \lambda^2 t e^{-\lambda t}$;
6. Using $f_c$ and $f_s$, Compute the failure rate of the entire
   network using $f_{rp} = \lambda(1 - G_F)e^{-\lambda t} + \lambda^2 G_F t e^{-\lambda t}$;
5. Using $f_{rp}$, Computer the CPC value using Erlang
   distribution through $CPC = (1 + G_F \lambda t)e^{-\lambda t}$;
6. End for
7. End
```

Fig. 3(a) illustrates the computation CPC in an ad hoc environment, in which the routing path is represented as S → 6 → 1 → 4 → 3 → 5 → D, where S and D are designated as source and destination nodes respectively. Here, node 1 is identified as selfish based on the value G_F. Our ECCPM approach estimates the impact of selfish node present in the routing path toward the resilience of the network through λ, f_c and f_s as CPC = 0.37.

Fig. 3(b) illustrates the computation CPC in an ad hoc environment, in which the routing path is represented as S → 6 → 1 → 4 → 3 → 5 → D, where S and D are designated as source and destination nodes respectively. Here, node 1, 4 and 3 are identified as selfish based on the value G_F. Our ECCPM approach estimates the impact of selfish nodes present in the routing path toward the resilience of the network through λ, f_c and f_s as CPC = 1.31.

3.5. Decision on Isolation of Selfish nodes based on CPC

The ECCPM approach isolates the selfish nodes based on computed CPC value. This CPC value quantifies the impact of selfish nodes toward the resilience of the network. If the CPC value is less than the resilience threshold, then the identified selfish node are isolated from the routing path to enable reliable data dissemination.

The algorithm 4 illustrates the steps regarding isolation of the identified selfish nodes from the routing path based on CPC.

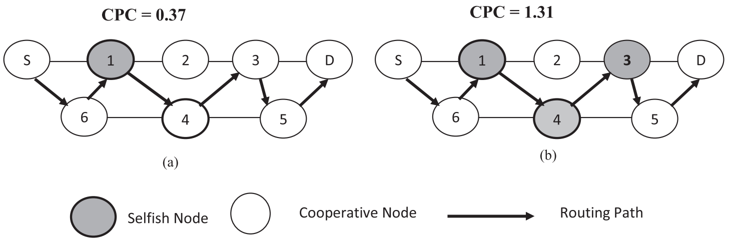


Figure 3 Estimation of CPC using ECCPM.

Algorithm 4: Decision on Isolation of Selfish nodes based on CPC. Notations

CPC – Conditional Probability Coefficient

RTh – Resilience Threshold.

Algorithm (Isolate Selfish Node)

```
1. Begin
2. For every routing path in the network
3. If (CPC  > RTh), then
4. Isolate selfish nodes using selfish _ Isolate ()
5. Else
6. Normal routing activity.
7. End for
8. End
```

Fig. 4, illustrates how ECCPM approach isolates the selfish nodes present in the routing path based on the value of CPC. The ECCPM approach computes the CPC value through λ, f_c and f_s values. Since the value of CPC is less than threshold resilience of the network, the identified selfish nodes 1, 4 and 3 in this scenario are isolated from the routing path for enabling reliable data dissemination. From the simulation study, the value of threshold of resilience is obtained as 0.60.

3.6. Correctness of the algorithm

In this section, we prove the correctness of ECCPM based on the requirements for isolating selfish nodes.

Proposition 1. *Our algorithm proves that any mobile node in the ad hoc environment will be selfish or cooperative.*

It is identified that, the implementation of algorithm 1 in an ad hoc environment, computes the genuineness factor for each and every node present in that scenario based on the second hand information such as probability of packet delivery, average packet delivery rate, normalized reputation factor obtained from neighbors. If the node has less probability of delivering the packets received by it, then the average packet delivery rate of that node is found to be minimum which in turn reduces the node's normalized reputation factor. When the value of normalized factor is less, it may result in minimum value of genuineness factor based on which the selfish nodes are identified. Hence, it is obvious that each and every mobile node in an ad hoc environment may exhibit selfish or cooperative behavior and this can be identified by means of second hand reputation.

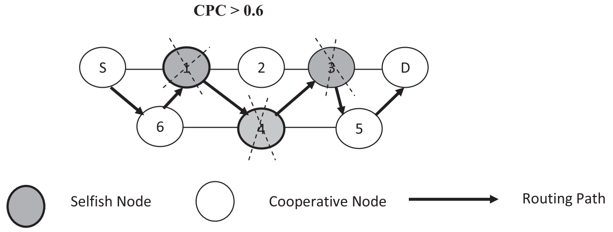


Figure 4 Isolating selfish nodes based on CPC.

Proposition 2. *Our algorithm proves that the presence of selfish node in the ad hoc environment produces a negative impact on the resilience of the network.*

It is identified that, the implementation of algorithm 2 in the ad hoc environment, counts the number of selfish nodes and cooperative nodes, based on which the non-cooperativity factor is calculated. The implementation of algorithm 3 calculates Conditional Probabilistic Coefficient (CPC) based on the non-cooperativity factor through Erlang distribution. This CPC value monotonically increases with the increase in number of selfish nodes in the network. Algorithm 4 isolates the selfish nodes, when the CPC value reaches above the resilience threshold, the point at which reliable dissemination of data is highly affected. Hence it is clear that the presence of selfish node may produce the negative impact toward the resilience of the network.

4. Simulation experiments and analysis

In this section, the performance and characteristics of the proposed ECCPM is studied via simulation. To compare the performance of ECCPM with the existing algorithms viz., RCSBMM, RFBMM, SHRCM, and PCMA, each them are stimulated with the same characteristics and network related parameters of ECCPM.

The reliable dissemination of data between source and destination highly depends on the cooperation established between the intermediate nodes (Eddy Cizeron and Salima Hamma, 2009), (Li et al., 2009), (Amir Khusru Akhtar and Sahoo, 2013).The selfish behavior of an intermediate mobile node may decrease the packet delivery rate, increase the packet drop rate and further may also increase the number of retransmissions of the network (Vaishampayan and Garcia-Luna-Aceves, 2004), (Viswanath et al., 2006), (Ruiz and Gomez-Skarmeta, 2004). Hence, the performance of the ECCPM is analyzed based on following performance metrics.

Packet Delivery Ratio (PDR): It is defined as the ratio of total number of packets received by the destination to the total number of packets destined to the receiver.

Throughput: It may be defined as the maximum number of data packets delivered at the destination node in a time instant.

Total Overhead: It may be defined as the ratio of number of packets required for establishing end to end communication between the source and destination node to the actual number of data packets received by the destination node.

Control Overhead: It may be defined as the maximum size of bytes that are required for establishing end to end connectivity between the source and destination nodes.

4.1. Simulation configuration

To simulate the algorithms, suitable simulation parameters are identified and tabulated in Table 1.

4.2. Results and discussion

The simulation results show that maximum number of selfish nodes are identified, when the genuineness factor set for detection is 0.30 (saddle point) compared to RCSBMM, RFBMM, SHRCM and PCMA. Fig. 5 portrays the comparative analysis carried out in identifying the number of selfish nodes by varying the values set for detection (Genuineness Factor) for five mitigation mechanisms such as ECCPM, RCSBMM, RFBMM, SHRCM and PCMA.

It is evident that ECCPM identifies maximum number of selfish nodes when the detection range is in between 0.25 and 0.35. Hence 0.25 and 0.35 is considered to be the maximum and minimum threshold point for selfish node detection respectively.

4.2.1. Performance analysis of ECCPM based on saddle point set for detection

In our simulation experiment, the number of mobile nodes is varied from 20 to 100 and the saddle point set for detecting selfish nodes is set as 0.30. In each and every scenario, the ECCPM is analyzed by considering 7% of the mobile nodes as selfish nodes. The Figs. 6(a)–(d) shows the packet delivery ratio, throughput, total overhead and control overhead for the ECCPM, RCSBMM, RFBMM, SHRCM and PCMA.

Fig. 6(a) presents the packet delivery ratio for varying number of mobile nodes involved in data transmission. The PDR decreases with increase in number of mobile nodes participating in the data transmission. This decrease in PDR is due to the insufficient availability of bandwidth since enormous amount of data is generated when the number of transmitting nodes increases in the ad hoc environment. However, ECCPM exhibits an improved packet delivery rate than RCSBMM, RFBMM, SHRCM and PCMA at the saddle point of 0.30. Further, ECCPM shows an improvement of 9–15% in PDR than RCSBMM, from 11% to 17.2% than RFBMM, from 14% to 26% than SHRCM and from 18.2% to 28% than PCMA. Furthermore, ECCPM in an average shows a phenomenal improvement of 23.5% in packet delivery ratio.

Table 1 Simulation parameters.

Parameter	Value
NS Version	2.26
Number of nodes	100
Protocol used	AODV
Mac layer	802.11
Terrain area	1000 × 1000
Mobility model	Random way point
Simulation time	100 s
Traffic model	CBR (40 packets/s)
Packet size	512 bytes
Type of antenna	Antenna/Omni antenna
Type of Propagation	Two way Ground
Channel capacity	2 Mpbs
Refresh interval time	10 s

Fig. 6(b) shows the throughput for the given number of mobile nodes participating in data transmission. The throughput of the network decreases with increase in number of transmitting nodes. Since, the cumulative number of packets dropped per second increases with increase in number of transmitting nodes. But still, ECCPM increases the throughput of the network when compared to the RCSBMM, RFBMM, SHRCM and PCMA. It is evident that, the ECCPM shows an increase of 8% to 13% in throughput than the RCSBMM, from 15% to 19% than RFBMM, 19% to 23% than SHRCM and from 21% to 27% than PCMA. It is also clear that ECCPM, in an average of 21% increases the throughput of the network.

Fig. 6(c) and (d), represent the plots for total overhead and control overhead based on varying number of mobile nodes in an ad hoc environment. An increase in the number of mobile nodes increases the number of computations and transmissions which in turn increases the total overhead and control overhead. But ECCPM exhibits a reduction of 17% to 21% than RCSBMM, from 20% to 25% than RFBMM, from 23% to 29% than SHRCM and from 24% to 32% than PCMA. Similarly, ECCPM also demonstrates the reduction of 13% to 16% in control overhead than RCSBMM, from 17% to 21% than RFBMM, from 22% to 27% than SHRCM and from 23% to 29% over PCMA. In addition to this, results also confirm that ECCPM in average reduces the total overhead and control overhead by 26.4% and 23.6% respectively.

4.2.2. Performance analysis of ECCPM based on minimum threshold detection point of selfishness

In the simulation experiment 2, the performance of ECCPM is studied by varying the number of mobile nodes from 20 to 100 with the minimum threshold detection point of selfishness as 0.35. The Fig. 7(a)–(d) demonstrate the plots of packet delivery ratio, throughput, total overhead and control overhead for the ECCPM, RCSBMM, RFBMM, SHRCM and PCMA.

With regard to packet delivery ratio, ECCPM outperforms the RCSBMM, RFBMM, SHRCM and PCMA, even when the point of detection is set as 0.35 which is greater than the saddle point of detection (0.30). In each and every scenario, the ECCPM is analyzed by considering 7% of the mobile nodes as selfish nodes. Since, ECCPM isolates selfish nodes at the rate of 16% at 0.35 which is comparatively lower than the detection rate at 0.30. Fig. 7(a) shows that ECCPM improves the PDR from 7% to 13% than the RCSBMM, from 9% to14.2% than RFBMM, from 18% to 26% than SHRCM and from 24.2% to 33.8% than PCMA. In addition, ECCPM in an average demonstrates a significant improvement of 22.2% in packet delivery ratio.

Likewise, ECCPM significantly increases the throughput than RCSBMM, RFBMM, SHRCM and PCMA at the

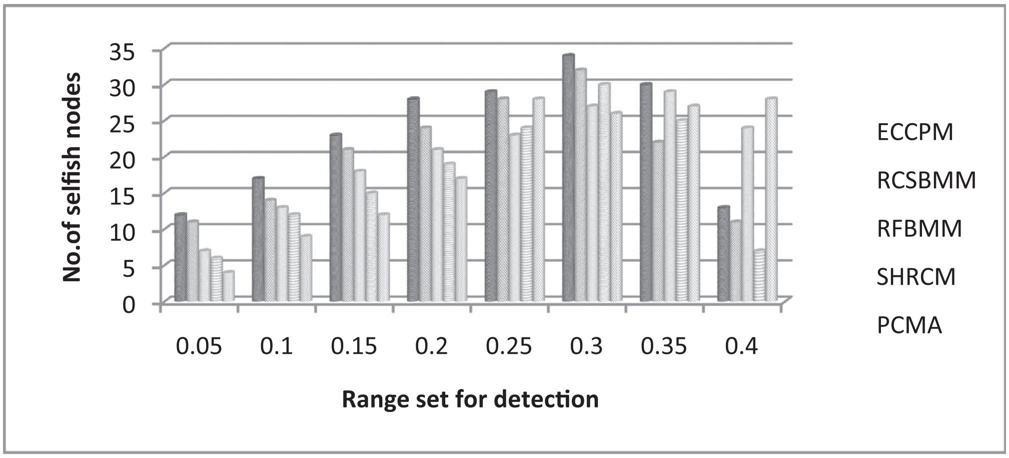


Figure 5 Comparative chart for identifying saddle point of selfish detection.

minimum threshold point of 0.35, since, ECCPM isolates considerable number of selfish nodes at 0.35. However, throughput achieved by ECCPM at a minimum threshold point of detection is comparatively less than the throughput exhibited at saddle point of detection. From Fig. 7(b) it is obvious that ECCPM increases throughput from 6% to 9%than the RCSBMM, from 13% to 17% than the RFBMM, from 16% to 21% than SHRCM and from 18% to 24% than PCMA. Further, it is also evident that ECCPM increases the throughput of the network at an average rate of 17%.

Further, ECCPM substantially reduces the control overhead and total overhead when compared to RCSBMM, RFBMM, SHRCM and PCMA at the minimum threshold point of detection. But, the reduction rate of overheads at 0.35 is lower when compared to percentage reduction of overheads at the saddle point. Furthermore, from Fig. 7(c), it is clear that ECCPM shows a decrease in total overhead from 15% to 19% than RCSBMM, from 17% to 23% than RFBMM, from 19% to 26% than SHRCM and from 21% to 29% over PCMA. Similarly, from Fig. 7(d), it is also evident that, ECCPM reduces control overhead from 11% to 15% than RCSBMM, from 13% to 17% than RFBMM, from 16% to 20% than SHRCM and from 23% to 28% over PCMA. Comprehensively, ECCPM reduces the total overhead and control overhead at an average rate of 24.4% and 20.6% respectively.

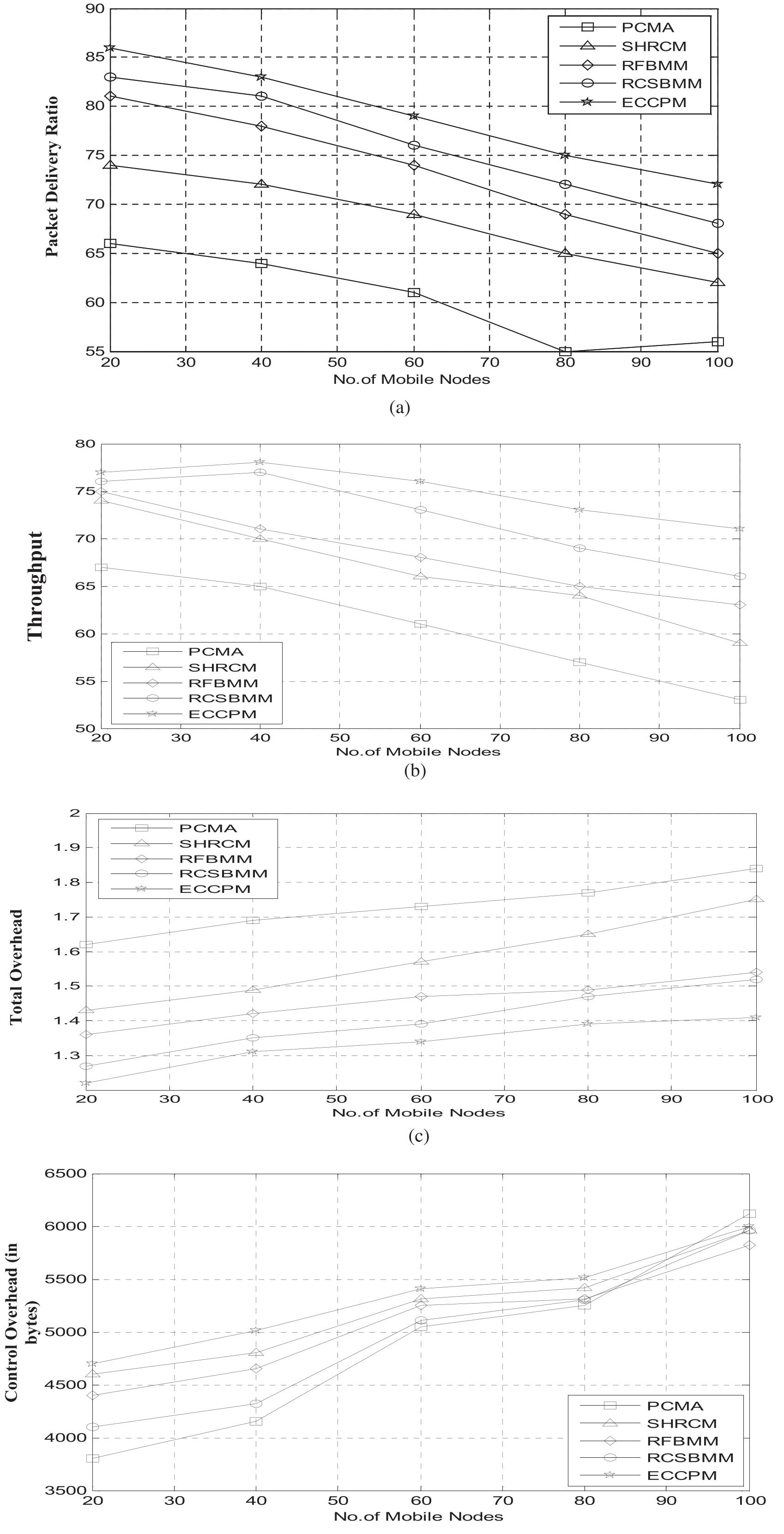
4.2.3. Performance analysis of ECCPM based on maximum threshold detection point of selfishness

In simulation experiment 3, the performance of ECCPM over RCSBMM, RFBMM, SHRCM and PCMA with maximum threshold detection point of 0.25 by varying the number of mobile nodes. In each and every scenario, the ECCPM is analyzed by considering 7% of the mobile nodes as selfish nodes. At this point, ECCPM exhibits an improved performance in terms of packet delivery ratio and throughput. However, the results indicate that, this significance of improvement incorporated by ECCPM at this point of detection is slightly higher than the performance shown at the minimum point of selfish detection and at the same time, it does not demonstrate an optimal improvement in performance as its behavior in 0.30. From Fig. 8(a), it is obvious that, ECCPM increases the PDR from 9% to 14.2% than the RCSBMM, from 10% to 16.2% than RFBMM, from 19% to 28% than SHRCM and from 24.4% to 25% than PCMA. Likewise, from Fig. 8(b) it is clear that, ECCPM increases the throughput from 7% to 11% than RCSBMM, from 15% to 19% than RFBMM, from 18% to 23% than SHRCM and from 18% to 24% than PCMA. In addition, it is observed that, ECCPM in an average improves the PDR and throughput by 24.4% and 18.2% respectively.

Further, results indicate that, ECCPM significantly improves the network performance by decreasing the total overhead and control overhead at the maximum threshold point of detection. Since, the number of retransmissions decreases at this point, the performance of ECCPM is slightly higher than at the minimum threshold point of detection. The Fig. 8(c), portrays that ECCPM reduces the total overhead from 17% to 22% than RCSBMM, from 19% to 26% than RFBMM, from 19% to 26% than SHRCM and from 24% to 32% than PCMA. The Fig. 8(d), illustrates that the ECCPM reduces the control overhead from 13% to 19% than RCSBMM, from 15% to 19% than RFBMM, from 19% to 23% than SHRCM and from 26% to 31.2% over PCMA. Hence, it is obvious that ECCPM is an effective algorithm in reducing the total overhead at an average rate of 26.2% and 22.4% respectively.

Furthermore, the performance of ECCPM is studied by varying the number of selfish nodes. Results presented in the Fig. 9(a) and 9(b) further confirm that the packet delivery ratio and throughput decreases when the number of selfish nodes are increased from 5 to 25 proportionally in increments of 5, since, an increase in the number of selfish nodes in an ad hoc environment increases the amount of packets dropped by the mobile nodes.

Finally, the proposed ECCPM approach is further analyzed by varying the threshold point of selfish node detection (especially with the threshold points of 0.40 and 0.50). At the detection point of 0.40, ECCPM improves the packet delivery ratio and throughput at an average rate of 16% and 14% respectively and at the same time, it reduces total overhead and control overhead by 18% and 19.6% respectively. Whereas, at the detection point of 0.50, ECCPM shows only a marginal improvement of 9% and 12% in terms of PDR



(a)

(b)

(c)

(d)

Figure 6 Comparison of ECCPM approach with RCSBMM, RFBMM, SHRCM and PCMA based on (a) Packet delivery ratio, (b) Throughput, (c) Total overhead, (d) Control overhead.

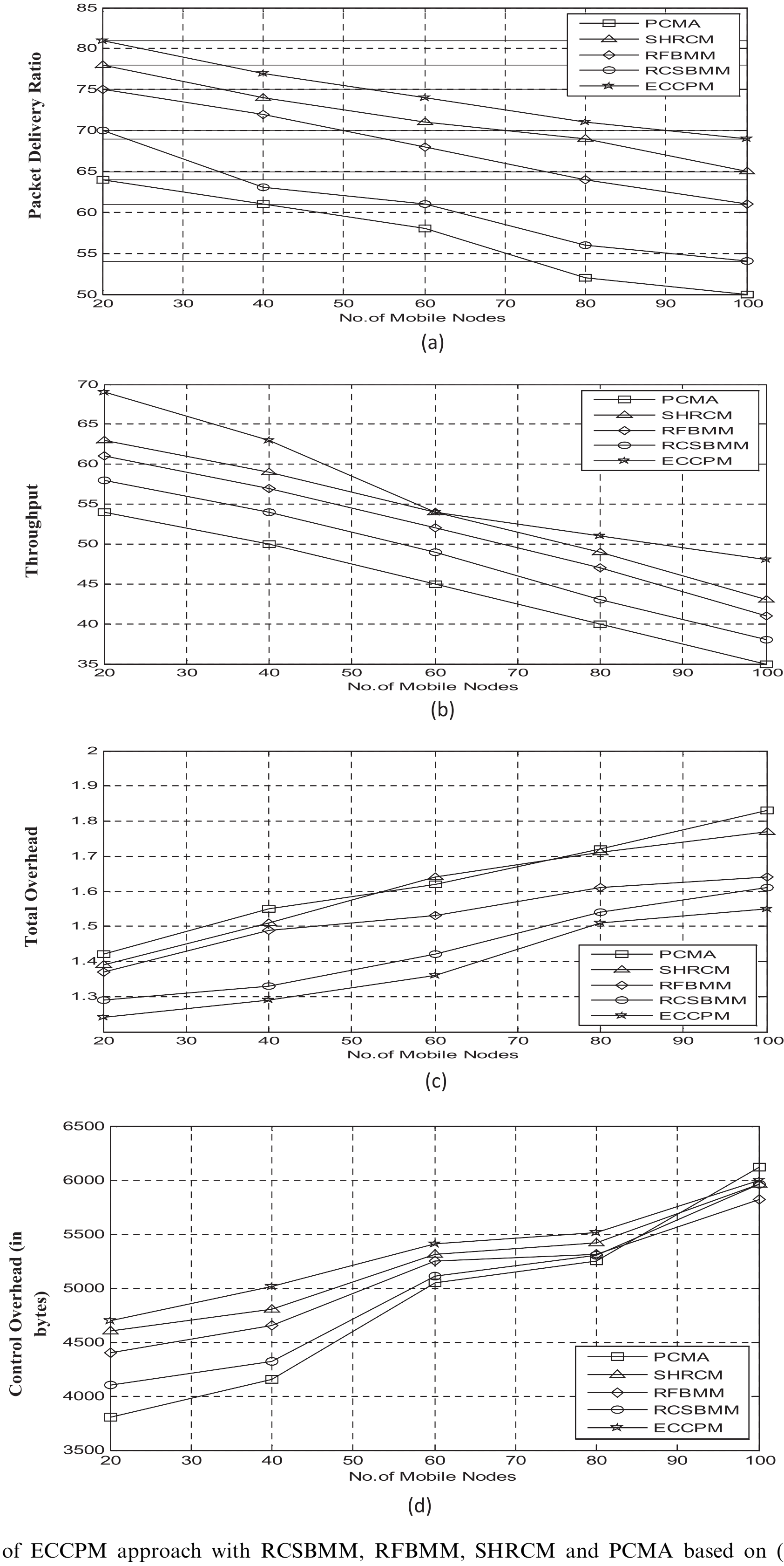
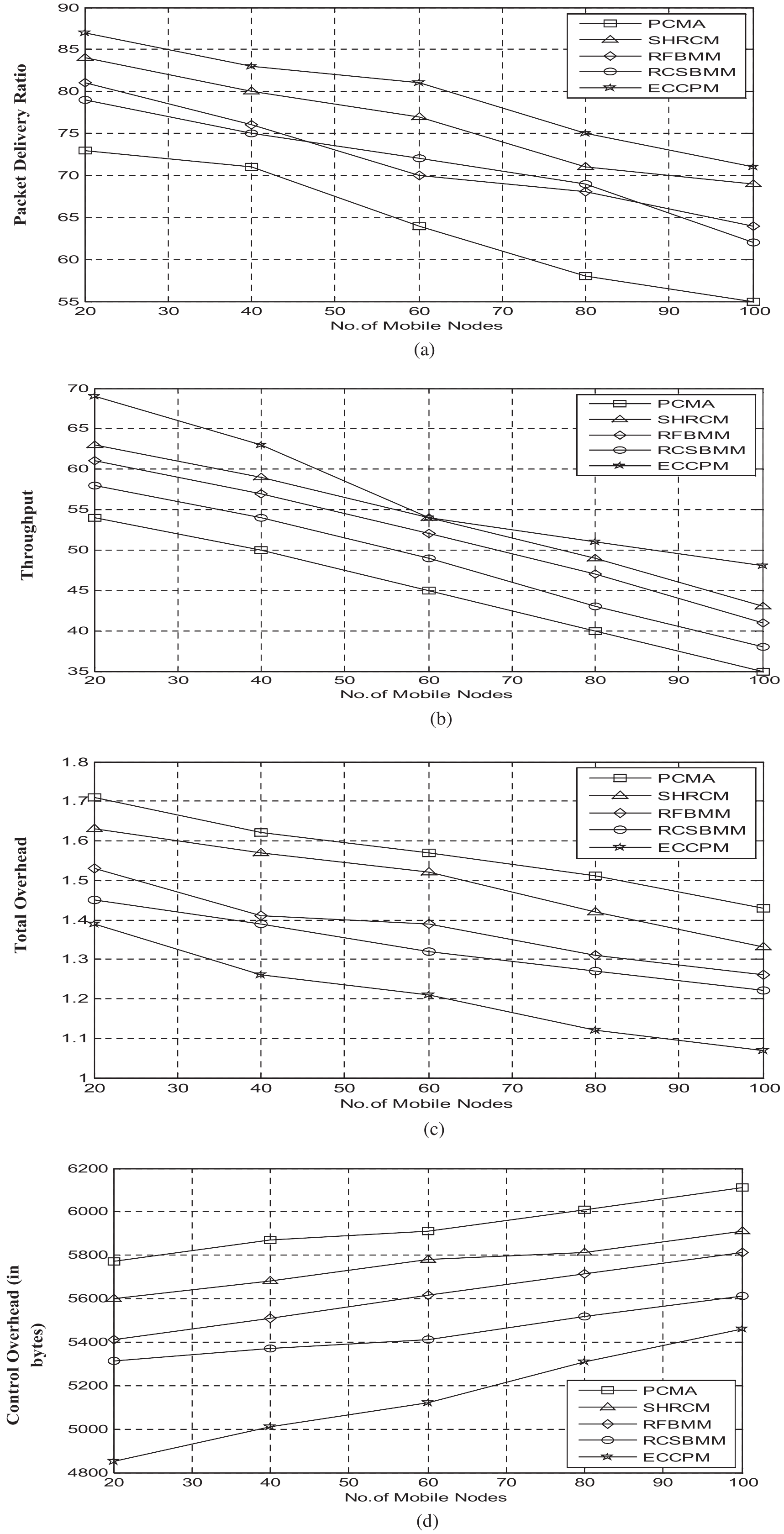


Figure 7 Comparison of ECCPM approach with RCSBMM, RFBMM, SHRCM and PCMA based on (a) Packet delivery ratio, (b) Throughput, (c) Total overhead, (d) Control overhead.



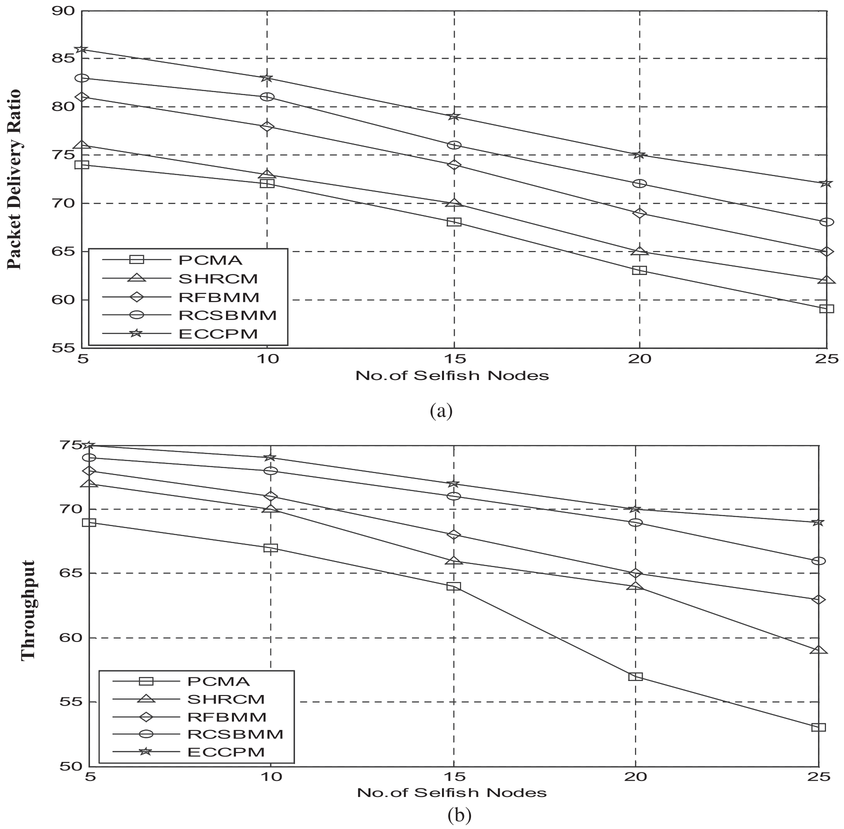
(a)

(b)

(c)

(d)

Figure 8 Comparison of ECCPM approach with RCSBMM, RFBMM, SHRCM and PCMA based on (a) Packet delivery ratio, (b) Throughput, (c) Total overhead, (d) Control overhead.



(a)

(b)

Figure 9 Comparison of ECCPM approach with RCSBMM, RFBMM, SHRCM and PCMA based on (a) Packet delivery ratio, (b) Throughput by varying the number of mobile nodes.

and throughput respectively. Similarly, it marginally improves the network performance by reducing the total overhead and control overhead by 14% and 12.4% respectively. Hence, we conclude that ECCPM exhibits an optimal performance only at the saddle point of detection (0.30).

5. Conclusion

This paper has presented an Erlang coefficient based conditional probabilistic model for detecting and isolating selfish mobile nodes in an ad hoc network. This ECCPM approach quantifies the impact of selfish nodes toward the resilience of the network, which in turn aids in framing a network resilience threshold of 0.60. The performance of ECCPM is analyzed based on packet delivery ratio, throughput, total overhead and control overhead by considering a saddle point of 0.30. Our ns-2 based simulation study makes it evident that, ECCPM in average improves the packet delivery ratio and throughput by 22.2% and 17% respectively and at the same time, ECCPM reduces the control overhead and total overhead by 24.4% and 20.6% respectively when compared to existing approaches suchas RCSBMM, RFBMM, SHRCM and PCMA. This is due to the rapid isolation rate of 23% incorporated by ECCPM based on the manipulation of Conditional Probabilistic Coefficient. Further, it is also evident that, ECCPM outperforms the existing approaches at the minimum threshold detection point of 0.25 and the maximum threshold detection point of 0.35. As a part of our future work, we have been planning to devise a rebuilding mechanism based on a reputation that could facilitate a node to get reinstituted in the network, which has been identified as selfish and isolated from the network.

References

Amir Khusru Akhtar, Md., Sahoo, G., 2008. Mathematical model for the detection of selfish nodes in MANETs. Int. J. Comput. Sci. Inf. 1 (3), 25–28.

Amir Khusru Akhtar, Md., Sahoo, G., 2013. Classification of selfish and regular nodes based on reputation values in MANET using adaptive decision boundary. Sci. Res. J. Commun. Networks 5 (1), 185–191.

Annapourna, P.Patil, Kanth, Rajani, Bathey Sharanya, M.P., Dinesh Kumar, M.P., Malavika, J., 2011. Design of energy efficient routing protocols for MANETs. Int. J. Comput. Sci. Issues 8 (1), 215–220.

Binglai Niu, H., Zhao, Vicky, Jiang, Hai., 2011. A cooperation stimulation strategy in wireless multicast networks. IEEE Tran. Signal Process. 59 (5), 2355–2369.

Bo Wang, Sohraab Soltani, Jonathan Shapiro, K., Pang – Ning Tan, 2005, Local detection of selfish routing behavior in Ad hoc networks. In: Proc., 8th IEEE International Conference on Parallel Architectures, Algorithms and Networks, vol. 1, no. 1, pp. 16–22.

Buchegger, S., Boudec, J.-Y. 2002a. Nodes bearing Grudges: towards routing security, fairness, and robustness in mobile Ad-Hoc networks. In: Proc., at Tenth Eurominicro Workshop on Parallel, Distributed and Network based Processing, Canary Islands, Spain, vol. 1, no. 1, pp. 234–242.

Buchegger, S., Boudec, J.-Y., 2002b. Performance Analysis of the CONFIDANT protocol: cooperation of nodes – fairness in distributed Ad-hoc networks. In: Proc., 3rd ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc '02), New York, USA, vol. 1, no. 1, pp. 226–236.

Buttyan, L., Hubaux, J.-P., 2003. Stimulating cooperation in self–organizing mobile Ad hoc networks'. MONET J. Mobile Comput. Networking 8 (1), 579–592.

Chen, T.M., Varatharajan, V., 2009. Dempster-shafer theory for intrusion detection in ad hoc networks. IEEE Internet Comput. 3 (1), 234–241.

Eddy Cizeron, Salima Hamma, 2009. Multipth routing in MANETs using multiple description coding. In: IEEE International Conference on Wireless nd Mobile Computing, Networking and Communications, vol. 1, no. 1, pp. 282–287.

Eidenbenz, Stephan, Resta, Giovanni, Santi, Paolo, 2008. The COMMIT protocol for truthful and cost – efficient routing in ad hoc networks with selfish nodes. IEEE Trans. Mob. Comput. 7 (1), 19–33.

Tarag Fahad, Robert Askwith, 2006, A node misbehaviour detection mechanism for mobile ad hoc networks'. In: Proc., Seventh Annual Post Graduate Symposium on the convergence of Telecommunications, Networking and Broadcasting (PGNet), vol. 1, no. 1, pp. 78–84.

Khalaf, Gamal Abdel Fadeel Mohamed, Badr, Hesham Zarief, 2013. A comprehensive approach to vertical handoff in heterogeneous wireless networks. J. King Saud Univ. Comput. Inf. Sci. 25 (1), 197–205.

Hernandez-Orallo, E., Manuel Serraty, D., Juan-Carlos, Cano, Juan-Carlos, Cano, Calafate, T., Manzoni's, P., 2012. Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Commun. Lett. 16 (5), 123–131.

Hongxun Liu, Jose, G., Delgado-Frias, Srisha Meddi, 2007. Using two-timer scheme to detect selfish nodes in mobile ad-hoc networks. In: Proc., 6th International Conference on Communication, Internet and Information Technology, Alberta, Canada, vol. 1, no. 1, pp. 179–184.

Kargl, F., Klenk, A., Schlott, S., Weber, M., 2004. Advanced detection of selfish or malicious nodes in ad hoc networks. In: Proc., First European Workshop on Security in Ad-Hoc and Sensor Network (ESAS 2004), Heidelberg, Germany, vol. 1, no. 1, pp. 255–263.

Abood Omer, Khaled Ahmed, 2009. Analytical study of MFR routing algorithm for mobile ad hoc networks. J. King Saud Univ. Comput. Inform. Sci. 22 (1), 105–113.

Komali, Ramakant S., MacKenzie, Allen B., Gilles, Robert P., 2008. Effect of selfish node behavior on efficient topology design. IEEE Trans. Mob. Comput. 7 (9), 1057–1070.

Laoutaris, Nikolaos, Smaragdakis, Georgios, Bestavros, Azer, Matta, Ibrahim, Stavrakakis, Loannis, 2007. Distributed selfish caching. IEEE Trans. Parallel Distrib. Syst. 16 (10), 1362–1375.

Li, Z., Jia, Z., Zhang, R., Wang, H., 2009. Trust-based on-demand multipath routing in mobile ad hoc networks, special issue on multi agents and distributed information security. IET Inf. Secur. 4 (4), 212–232.

Marti, S., Gulli, T.J., Lai, K., Baker, M., 2000. Mitigating routing misbehavior in mobile ad hoc networks Mobile Computing and Networking. In: Proc., 6th ACM Annual International Conference on Mobile Computing and Network (ACM-MobiCom), Boston, USA, vol. 1, no. 1, pp. 255–265.

Michiardi, P., Molva, R., 2002. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks'. In: Proc., 6th IFIP Conf. on Security, Communications and Multimedia, Protoroz, Solvenia, vol. 228, no. 1, pp. 107–121.

Paul, K., Westhoff, D., 2002, Context aware detection of selfish nodes in DSR based ad hoc networks. In: Proc., IEEE Globecom, vol. 1, no. 1, pp. 456–462.

Rizvi, S., Elleithy, M., 2009. A new scheme for minimizing malicious behavior of mobile nodes in Mobile Ad Hoc Networks'. Int. J. Comput. Sci. Inform. Secur. 3 (1), 25–34.

Ruiz, P.M., Gomez-Skarmeta, 2004. Reducing data overhead of mesh based ad hoc multicast routing protocols by steiner tree meshes. In: Proc., of IEEE SECON, vol. 4, no. 7, pp. 54–62.

Sengathir, J., Manoharan, R., 2013a, Selfish Conscious Mathematical Model based on Reliable Conditional Survivability Co efficient in MANET Routing. In: Proc., 3rd Third International Conference on Advances in Information Technology and Mobile Communication, (AIM 2013) Bangalore, India, vol. 1, no. 1, pp. 31–40.

Sengathir, J., Manoharan, R., 2013b. A split half reliability coefficient based mathematical model for mitigating selfish in MANETs. In: Proc., 3rd IEEE International Advance Computing Conference (IACC-2013), Ghaziabad, India, Feb 22–23, 2013, IEEE vol. 1, no. 1, pp. 267–272.

Sengathir, J., Manoharan, R., 2014. A reliability factor based mathematical model for isolating selfishness in MANETs. Int. J. Inform. Commun. Technol. 6 (3/4), 403–421, Special issue on Recent Trends in Intelligent Computation and Communication System Design.

Senthilkumaran, T., Sankaranarayanan, V., 2013. Dynamic congestion detection and control routing in ad hoc networks. J. King Saud Univ. Comput. Inform. Sci. 25 (1), 25–34.

Dehnie, Sintanyehu, Tomasin, Stefano, 2010. Detection of selfish nodes in networks using CoopMAC protocol with ARQ. IEEE Trans. Wireless Commun. 9 (7), 2328–2337.

Vaishampayan, J.J Garcia-Luna-Aceves, 2004. Efficient and robust multicast routing in mobile ad hoc networks. In Proc., of the IEEE Conference on Mobile Ad-hoc and Senior system, 304–313, Oct 2004.

Viswanath, K., Obraczka, K., Tsudik, G., 2006. Exploring mesh and tree-based multicast routing in mobile ad hoc networks. IEEE Trans. Mob. Comput. 5 (1), 28–42.

Wang, Weizhao, Li, Xiang.-Yang, 2006. Low-Cost routing in selfish and rational wireless ad hoc networks. IEEE Trans. Mob. Comput. 5 (5), 596–607.

Yanwei, Wu, Tang, Shaojie, Ping, Xu, Li, Xiang-Yang, 2010. Dealing with selfishness and moral hazard in non-cooperative wireless networks. IEEE Trans. Mob. Comput. 9 (3), 420–434.

Khamayseh, Yaser, Obiedat, Ghadeer, Yassin, Munner Bani, 2011. Mobility and load aware routing protocol for ad hoc networks. J. King Saud Univ. Comput. Inform. Sci. 23 (1), 105–113.

Zouridaki, C, Mark, B.L., Hejmo M., Thomas R.K., 2009. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In: Proc., of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, vol. 1, no.1, pp. 1–10.