Egyptian Informatics Journal (2015) **16**, 231–241

Cairo University

Egyptian Informatics Journal

www.elsevier.com/locate/eij
www.sciencedirect.com

ORIGINAL ARTICLE

Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs

J. Sengathir *, **R. Manoharan**

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

Received 10 October 2014; accepted 23 May 2015
Available online 17 July 2015

KEYWORDS

Selfish nodes;
Exponential weighted moving average;
Residual power;
Power drain rate;
Exponential Reliability Coefficient

Abstract In mobile ad hoc networks, cooperation among active mobile nodes is considered to play a vital role in reliable transmission of data. But, the selfish mobile nodes present in an ad hoc environment refuse to forward neighbouring nodes' packet for conserving its own energy. This intentional selfish behaviour drastically reduces the degree of cooperation maintained between the mobile nodes. Hence, a need arises for devising an effective mechanism which incorporates both energy efficiency and reputation into account for mitigating selfish behaviour in MANETs. In this paper, we propose an Exponential Reliability Coefficient based reputation Mechanism (ERCRM) which isolates the selfish nodes from the routing path based on Exponential Reliability Coefficient (ExRC). This reliability coefficient manipulated through exponential failure rate based on moving average method highlights the most recent past behaviour of the mobile nodes for quantifying its genuineness. From the simulation results, it is evident that, the proposed ERCRM approach outperforms the existing Packet Conservation Monitoring Algorithm (PCMA) and Spilt Half Reliability Coefficient based Mathematical Model (SHRCM) in terms of performance evaluation metrics such as packet delivery ratio, throughput, total overhead and control overhead. Further, this ERCRM mechanism has a successful rate of 28% in isolating the selfish nodes from the routing path. Furthermore, it also aids in framing the exponential threshold point of detection as 0.4, where a maximum number of selfish nodes are identified when compared to the existing models available in the literature.

© 2015 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

* Corresponding author. Tel.: +91 9940808674.
E-mail addresses: j.sengathir@gmail.com (J. Sengathir), rmanoharan@pec.edu (R. Manoharan).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

1. Introduction

Mobile ad hoc network (MANET) is an autonomous system of mobile devices connected without a centralized infrastructure. Since, MANETs lack a centralized authority for communication, they rely upon the reputation level of the intermediate nodes for forwarding packets between the source

http://dx.doi.org/10.1016/j.eij.2015.05.003
1110-8665 © 2015 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

and destination. Further, the degree of reputation depends upon the rate of packets forwarded by a mobile node for its neighbour. Furthermore, the reputation level of each and every mobile node can be computed based on the first hand and second hand reputation mechanisms. In first hand reputation mechanism, the reputation level is derived through direct interaction from the mobile node. In contrast, the second hand reputation approach manipulates the reputation factor of a mobile node by quantifying the information elucidated from their neighbours [1].

In addition, a mobile ad hoc network is classified as open or closed based on user perspective in sharing the resources. In open MANETs, different mobile users with different goals share the resources for achieving cooperation which in turn induces effective communication [2]. But still, the open environment of MANET is highly vulnerable to misbehaving nodes and selfish nodes. In which, the misbehaving nodes intrudes into a network for compromising mobile hosts for exploiting network resources, while, the selfish nodes are termed as non-cooperative nodes that refuse to forward other nodes' packet in order to save their precious energy. These selfish nodes can be classified into three board categories [3] viz.,

- TYPE 1 – Selfish Nodes: These types of selfish nodes actively participate in route discovery and route maintenance process. But, refuses to forward the data packets for their neighbours.
- TYPE II – Selfish Nodes: These selfish nodes neither forward data nor participate in route discovery process.
- TYPE III – Selfish Nodes: These selfish nodes change their behaviour dynamically by dropping packets based on its residual energy.

The presence of TYPE–II selfish nodes is neglected by most of the routing protocols proposed for MANETs. In contrast, TYPE–I and TYPE–III selfish nodes are considered to be more crucial, since these nodes may interrupt the reliable transmission of data [4]. Hence, reputation mechanisms become essential for detecting and isolating TYPE–I and TYPE–III selfish nodes.

In this paper, we propose an Exponential Reliability Coefficient Based Reputation Mechanism (ERCRM) which detects and isolates selfish nodes based on estimated energy metric and Exponential Reliability Coefficient through the second-hand information obtained from their neighbours. This ERCRM is considered to be more effective and efficient since it incorporates both energy efficiency and packet forwarding nature of mobile nodes for mitigating selfishness. Further, ERCRM effectively mitigates TYPE–I and TYPE–III categories of selfish nodes and thus enhances the network performance.

This paper is intended to answer the following questions.

1. How could the energy level of a mobile node be utilized for identifying the selfish behaviour of mobile nodes?
2. What is the significance of Exponential distribution for quantifying the mobile nodes' reputation factor?
3. Whether the proposed model detects and isolates selfish nodes in an efficient and effective manner, when compared to the existing approaches?
4. How the proposed model could significantly aid in framing exponential threshold point for detection, the point at which maximum of number selfish nodes identified?

The remaining part of the paper is organized as follows. Section 2 presents the detailed discussion about the existing reputation based selfish node mitigation mechanisms with the shortcomings of the literature. Section 3 elaborates ERCRM approach to detect selfish nodes based on the computation of estimated energy metric and exponential reliability coefficient with their corresponding algorithms and illustrations. Section 4 describes the exhaustive simulation study conducted for evaluating the performance of ERCRM approach along with its results analysis and Section 5 concludes the paper with possible future research recommendations.

2. Related work

From the past decade, several new reputation mechanisms have been contributed to deal with the potential selfish nodes. Some of the competent approaches are enumerated below.

Marti et al. [5] proposed a reputation mechanism which incorporates watch-dog and path-rater for effective detection and mitigation of malicious nodes present in the ad hoc network. This mechanism detects malicious nodes based on two levels of rating obtained through the link level and forwarding level monitored by each and every mobile node. This mechanism also utilizes two rating levels namely suspected rating and neutral rating for identifying misbehaving nodes. Michardi and Molva [6] have proposed a collaborative reputation framework, which utilizes watch-dog as the detection component. Authors have utilized three reputation approaches viz., subjective reputation, indirect reputation and functional reputation for detecting selfish nodes. Authors also formulated a mechanism for detecting misbehaving nodes based on threshold level of packets dropped by a mobile node.

Further, Buchegger and Boudec [7], have proposed a novel reputation approach based on four entities namely trust manager, path manager, monitor and the reputation system which estimates the reputation level of each and every mobile node present in the ad hoc network through the first and second hand information. This approach is a distributed approach which maintains alarm table, trust table and friend list for detecting selfish nodes through the coordination of trust manager and pate manager. This mechanism also isolates the selfish nodes at the faster rate based on the component called monitor that continuously monitors the deviation of an individual node from its normal behaviour. Waing and Li [8] proposed a cooperative enforcement mechanism based on strategy proof pricing. This centralized algorithm further utilizes an optimal time for computing strategy proof based on least cost path.

Furthermore, Buttyan and Hubaux [9] proposed a tamper resistant model that incorporates high degree of collaboration among the mobile nodes by enforcing cooperation based on nuglet counter. This nuglet counter is used to estimate the malicious behaviour of the nodes, which gets monotonically increased and decreased based on the role played by the mobile nodes. This resistant model also induces a greater level of coordination between the mobile nodes by means of reward and

punishment strategies deployed in a distributed manner in each and every node. Kargl et al., [10] have contributed an evidence based mobile intrusion detection system that incorporates the capability of overhearing through an embedded secure architecture called SAM. This detection mechanism utilizes a routing protocol namely SDSM, that optimally decides the routing strategy through negotiation among the participating mobile nodes of the networks.

In addition, Farad and Askwith [11] proposed a Packet Conservation Monitoring Algorithm (PCMA) that aids in detecting the malicious nodes in the ad hoc scenario. This monitoring algorithm mainly targets on the detection of specific type of malicious nodes from the routing path and thus enables reliable dissemination of data by increasing the overall performance of the network in terms of packet delivery ratio, throughput, total overhead and control overhead. Zouridaki et al. [12] contributed a reputation mechanism for detecting malicious nodes based on opinion metric. This opinion metric is calculated based on trust and confidence limit estimated through the statistical values obtained from the reliable delivery of packets. Authors have considered both first hand and second hand reputation information for detecting maliciousness.

Rizvi and Elleithy [13] contributed a time division based approach for mitigating malicious behaviour of nodes. This approach clarified the ambiguity that exists between selfish behaviour and malicious behaviour of mobile nodes. They also proposed a cooperative and consistent trust mechanism for provisioning resource utilization. They also analyse the performance of the network through parameters such as network utilization and transmission overhead. Komali et al. [14] proposed a selfish mitigation approach that incorporates energy consumption and network connectivity into account. This mitigation mechanism integrates Max-improvement and Delta-improvement algorithm for isolating selfish nodes. This mechanism also utilizes Nash equilibrium properties for confirming selfishness.

Another class of effective mitigation mechanism in which mitigation is based on residual energy parameter of a mobile was presented by Binglai Niu et al. in [15]. Authors contribute an energy efficient routing mechanism based on AODV, which combines two different energy cost metrics into single quantity. This energy efficient mechanism was compared with AODVEA and LEAR mechanism proposed for energy efficient routing. Hernandez Orallo et al. [16] formulated a collaborative watchdog mechanism that detects the selfish behaviour based on transition probability matrix. This transition probability matrix consists of two entities called Q and R, which is needed for estimating the detection time and network overhead induced by the selfish nodes. This watchdog mechanism utilizes two states viz., NO INFO and POSITIVE for detecting selfish nodes based on constant time Markov chain. This mechanism is also ideally suited for manipulating the false positives and false negatives that could be caused during selfish node detection. Paul and Westhoff [17] investigated distributed mechanisms for mitigating selfish nodes in an ad hoc environment. Authors have analysed the presence of selfish nodes using a context aware reputation based mechanism.

Yet, Liu et al. [18] innovated a two-timer approach that detects selfish nodes by classifying packets into data packets and control packets. This categorization of packets was achieved by means of an entity called drop counter which gets updated periodically whenever a packet enters or leaves nodes. This mechanism identifies the mobile node as selfish when the drop counter exceeds a threshold value. Eidenbenz et al. [19] proposed a COMMIT protocol to prevent the exploitation of network utilization. This COMMIT protocol integrates game theoretic approach with VCG payment scheme for identifying misbehaving nodes. Dehnie and Tomasin [20] contributed a cooperative MAC protocol which performs uniformly powerful test and probability ratio test. From these tests conducted, the effect of fading and interference that could result due to the presence of selfish nodes in the ad hoc environment is further analysed.

Yet another, novel method for mitigating selfish through second hand reputation mechanism based on split half reliability coefficient was proposed by Sengathir and Manoharan [21].This mechanism estimates the nodes' behaviour with regard to two perspectives viz, packet delivery rate of a mobile node and packet forwarding ability of a mobile node. The split half reliability coefficient is derived based on Karl Pearson correlation coefficient and spearman brown formula that interprets the change in the level of nodes' behaviour from its normal routing activity.

Extract of the literature

The review on the reputation based approaches for mitigating selfish nodes present in the literature has the following limitations.

- An Exponential distribution based reputation mechanism which incorporates second hand information for mitigating selfish nodes has not been proposed to the best of our knowledge.
- A reputation approach which predicts the mobile nodes' behaviour by considering exponential time into account is not much explored.

Further, Exponential distribution is considered as the only continuous probability distribution, which independently monitors mobile nodes' behaviour at a constant average rate. Hence, it is motivated to formulate an Exponential distribution based reputation approach for isolating selfish nodes present in the ad hoc environment.

3. Exponential Reliability Coefficient based Reputation Mechanism (ERCRM)

3.1. Problem statement

In ERCRM, a group of mobile nodes having a unique identity are connected in an ad hoc environment which is considered as an undirected graph $G = (N, P)$, where N is a set of mobile nodes and P is the set of paths between mobile nodes. In order to accomplish the objective of detecting and isolating selfish mobile nodes, the following key points are considered. Initially, the amount of energy possessed by each and every mobile node is quantified as estimated energy metric of that node for detecting Type I and Type III selfish nodes. Secondly, the packet delivery rate of each and every mobile node is manipulated in terms of Exponential Reliability Coefficient through exponential distribution for reconfirming

the detection of Type I selfish nodes. Thirdly, Type III selfish nodes are isolated when the estimated energy metric fall below the energy threshold value required for a mobile node to exist in cooperative mode. Finally, the isolation of Type I selfish nodes from the active routing path is performed based on the analysis of both estimated energy metric and exponential reliability coefficient for enabling reliable data dissemination.

Further, ERCRM is a distributed mechanism for mitigating selfish nodes in which the reliability coefficient is computed in each and every mobile node rather than a centralized node. This distributed ERCRM mechanism certainly increases the overhead which is compared to be negligibly small and furthermore, it is experimentally tested and elaborated in Section 4.

3.2. Detection of Type I and Type III selfish nodes based on estimated energy metric (E_{est})

When a source node wants to forward packets to the destination node based on one-hop neighbours, the Estimated Energy Algorithm determines the energy level of the intermediate nodes in the routing path by considering the two parameters into account viz.,

(a) The residual power (R_p) of a mobile node, which is defined as the amount of energy initially available in the mobile node before connection establishment.
(b) Power drain rate – (P_{dr}) of a mobile node, which is defined as average loss of power due to the data transmissions that occur in various sessions 's'. Hence, the power drain rate of a mobile node can be manipulated by considering the loss of power due to data transmission in a two successive session say 's' and 's-1' using exponential weighted moving average method given by (1)

$$P_{dr} = \alpha \times P_{dr}(s) + (1 - \propto) P_{dr}(s-1) \tag{1}$$

where α is defined as the weighted average which is computed through the ratio of minimum energy (min_energy_req) required for transmitting data in a specified routing path to the minimum number of hops (min_*hops*) existing between the source and destination given by (2)

$$\alpha = (\text{min\_energy\_req})/(\text{min\_}hops) \tag{2}$$

From this, we define the estimated energy metric (E_{est}) of a mobile node as the ratio of residual power of a mobile node to the power drain rate at any instant of time 't' as given by (3)

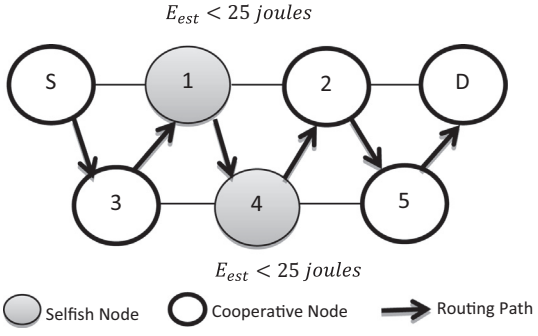

Figure 1 Detection of Type III selfish nodes based on Estimated Energy Metric (E_{est}).

$$E_{est} = \frac{R_p}{P_{dr}} \tag{3}$$

When the estimated energy (E_{est}) of a mobile node is determined to be less than the value of Energy threshold ($E_{thr} = 25$ joules), as proposed in [22], which is defined as the minimum energy required for a mobile node to participate in the routing activity. Then, the mobile node is designated as selfish. The following algorithm 1 illustrates the steps to estimate the Estimated Energy Metric (E_{est}) for each and every mobile node participating in the routing activity and further, from the estimated value of E_{est}, the behaviour of the node is categorized either as Type I or Type III selfish.

Algorithm 1: Manipulation of the Estimated Energy Metric (E_{est})

Notations:
n – represents the mobile node
S – Source node
D – Destination node
R_P – Residual Power
P_{dr} – Power Drain Rate
α– weighted Average
E_{est}– Estimated Energy Metric
E_{thr} – Energy Threshold
E_{min} – Minimum energy required for transmitting the data
H_{min} – No. of hops existing between source and destination

Algorithm (Estimation Energy Metric)
1. For each mobile node n_i in Network N,
2. if $n_i \in$ *Routing path* $(S, n_1, \ldots, n_m, d)$
   Set $R_p \leftarrow$ *Energy* (n_i), otherwise $R_p \leftarrow 0$
3. Compute, the weighted average α as $\frac{E_{min}}{H_{min}}$
4. Compute Power Drain Rate through
   $P_{dr} = \alpha \times P_{dr}(s) + (1 - \propto) P_{dr}(s-1)$
5. Compute the Estimated Energy Metric as
   $E_{est} = R_p / P_{dr}$
6. *if*$(E_{est} < E_{thr})$
   Assign each node $n_i(selfishness) \leftarrow true$, otherwise
   $n_i(selfishness) \leftarrow false$.
7. End for
8. While $n_i(selfishness) \leftarrow true$,
9. Call *selfishisolate*(n_i)
10. End While
11. End

Fig. 1 illustrates the computation of estimated energy metric for each and every mobile nodes participating in a routing path represented as $S \rightarrow 3 \rightarrow 1 \rightarrow 4 \rightarrow 2 \rightarrow 5 \rightarrow D$, where S represents the source node and D represents the destination node. In the above specified scenario, nodes 1 and 4 are identified to exhibit Type I or Type III selfish behaviour when the value of $E_{est} < 25$ joules.

3.3. Reconfirming the identification of Type I selfish nodes based on Exponential Reliability Coefficient (*ExRC*)

The mobile nodes which are identified as Type I selfish nodes using Estimated Energy Metric are further analysed through Exponential Reliability Coefficient ($ExRC$) for reconfirming Type I selfish nodes. This Exponential Reliability Coefficient is computed as follows.

Let '*rp*' be the number of packets received by the mobile node and '*fp*' be the number of packets forwarded by that mobile node to its next hop neighbour. Then, the packet drop (D_p) of the mobile node can be calculated based on number of packets dropped by that mobile node, as given by (4)

$$D_p = rp - fp \tag{4}$$

Similarly, the packet dropped by a mobile node as viewed in '*s*' sessions is calculated as $D_{p1}, D_{p2}, \ldots, D_{ps}$ respectively. Then, the packet drop rate estimated for a mobile node is manipulated through (5)

$$DR_p = D_{pi}/s \tag{5}$$

where $1 \leqslant i \leqslant s$

From the value of packet drop rate, DR_p the estimated Exponential Failure Rate (ERF) using moving average method is computed by (6)

$$ERF = \frac{\sum_{i=1}^{s} DR_{pi} \times P_i}{\sum_{i=1}^{s} P_i} \tag{6}$$

where P_i indicates the priority factor, which is calculated based on packet routing and acknowledgement approaches proposed for ad hoc network as presented in [23]. It is also considered as an important parameter utilized by the moving average method for projecting the most recent behaviour of the mobile nodes in order to estimate ERF.

This priority factor (P_i) for each and every session '*i*' is determined using (7),

$$P_i = w(R_{req}) \times R_{req} + w(R_{rep}) \times R_{rep} + w(R_{err}) \times R_{err} + w(D_{Pt}) \times D_{pt} \tag{7}$$

where $R_{req}, R_{rep}, R_{err}, D_{Pt}$ are the normalized deviations factors of route request, route reply, route error and data packets respectively. While, $w(\cdot)$ denotes the weight assigned for each and every successful event of delivering (i) route request acknowledgement packet (R_{req_s}) (ii) route reply acknowledgement packet (R_{rep_s}) (iii) route error acknowledgement packet (R_{err_s}) (iv) data packet (D_{pt_s}) and failure event of delivering (i) route request acknowledgement packe (R_{req_f}) t (ii) route reply acknowledgement packet (R_{rep_f}) (iii) route error acknowledgement packet (R_{err_f}) (iv) data packet (D_{pt_f})

$$R_{req} = \frac{R_{req\_s} - R_{req\_f}}{R_{req\_s} + R_{req\_f}} \tag{8}$$

$$R_{rep} = \frac{R_{rep\_s} - R_{rep\_f}}{R_{rep\_s} + R_{rep\_f}} \tag{9}$$

$$R_{err} = \frac{R_{err\_s} - R_{err\_f}}{R_{err\_s} + R_{err\_f}} \tag{10}$$

$$D_{pt} = \frac{D_{pt\_s} - D_{pt\_f}}{D_{pt\_s} + D_{pt\_f}} \tag{11}$$

Then, the exponential reliability coefficient $ExRC$ is manipulated using exponential distribution from ERF using (12)

$$ExRC = e^{-ERF} \tag{12}$$

The ERCRM approach reconfirms a mobile node as Type I selfish node based on the value of Exponential Reliability Coefficient ($ExRC$). If the determined value of $ExRC$ of a mobile node is found to be less than the exponential threshold value 0.40 (obtained through simulation as presented in Fig. 4), then the intermediate nodes are identified as Type I selfish nodes.

The following algorithms 2 and 3 illustrate the steps for computing priority factor in order to estimate Exponential Reliability Coefficient ($ExRC$) for reconfirming Type I selfish nodes. If a mobile node is identified as Type I selfish through algorithms 2 and 3, then the Selfish Isolation algorithm is called to isolate the selfish node from the routing path.

Algorithm 2: Computation of Priority Factor (P_i)

Notations:

n – represents the mobile node
P_i – Priority factor
R_{req} – Normalized route request deviation factor
R_{rep} – Normalized route reply deviation factor
R_{err} – Normalized route error deviation factor
D_{pt} – Data delivery deviation factor
R_{req_s} – Successful route request acknowledgement packet
R_{req_f} – Failure route request acknowledgement packet
R_{rep_s} – Successful route reply acknowledgement packet
R_{rep_f} – Failure route reply acknowledgement packet
R_{err_s} – Successful route error acknowledgement packet
R_{err_f} – Failure route error acknowledgement packet
D_{pt_s} – Successfully delivered data packet
D_{pt_f} – Failed data packets

Algorithm (Priority Factor (P_i))

1. For each mobile node n_i in the Network N,
2. For every session i, $i \in \{1, \ldots, s\}$
3. Compute $R_{req} = \frac{R_{req\_s} - R_{req\_f}}{R_{req\_s} + R_{req\_f}}$
4. Compute $R_{rep} = \frac{R_{rep\_s} - R_{rep\_f}}{R_{rep\_s} + R_{rep\_f}}$
5. Compute $R_{err} = \frac{R_{err\_s} - R_{err\_f}}{R_{err\_s} + R_{err\_f}}$
6. Compute $D_{pt} = \frac{D_{pt\_s} - D_{pt\_f}}{D_{pt\_s} + D_{pt\_f}}$
7. Find the Priority Factor using
$P_i = w(R_{req}) \times R_{req} + w(R_{rep}) \times R_{rep} + w(R_{err}) \times R_{err} + w(D_{Pt}) \times D_{pt}$
8. End for (each session)
9. End for (each mobile node)
10. End.

Algorithm 3: Computation of Exponential Reliability Coefficient ($ExRC$)

Notations:

n – represents the mobile node
rp –Number of packets received by the mobile node
fp – Number of packets forwarded by the mobile node
D_P – Number of packet dropped by a mobile node
DR_P – Packet drop rate
P_i – Priority Factor
ERF – Exponential Failure Rate
$ExRC$ – Exponential Reliability Coefficient

Algorithm (Exponential Reliability Coefficient)

1. For each mobile node n_i in Network N,
2. For every session j, $j \in (1, \ldots, s)$
3. Find the number of packets dropped by the mobile node through $D_p(n_i) \leftarrow Difference(rp, fp)$
   if $n_i \in Routing path(S, n_1, \ldots, n_m, d)$
   Otherwise $D_p(n_i) \leftarrow 0$
4. Compute the packet drop rate of the mobile node n_i as $DR_p(n_i) = D_{pi}/s$

5. End For
6. Calculate the exponential failure rate as
$ERF = \frac{\sum_{i=1}^{s} DR_{pi} \times P_i}{\sum_{i=1}^{s} P_i}$
7. Compute the exponential reliability coefficient through
$ExRC = e^{-ERF}$
8. *if*$(ExRC < 0.4)$
Assign each node $n_i(selfishness) \leftarrow true$, otherwise
$n_i(selfishness) \leftarrow false$.
9. End for
10. While $n_i(selfishness) \leftarrow true$, do
11. Call $selfishisolate(n_i)$
12. End While
13. End

Fig. 2 illustrates the computation of *ExRC* for each and every node in the routing path which is represented as $S \rightarrow 3 \rightarrow 1 \rightarrow 4 \rightarrow 2 \rightarrow 5 \rightarrow D$, where S and D represent the source and destination node respectively. In the above illustrated scenario, nodes 1 and 3 are identified to exhibit Type I selfish behaviour node based on the value *ExRC*.

3.4. Isolation of selfish nodes from the routing path

Algorithm 4: Isolation of selfish nodes from the routing path

Notation:
n – represents the mobile node

Algorithm (Selfish Isolation)
1. Begin
2. For every routing path in the network
3. While $n_i(selfishness) \leftarrow true\, do$
4. Discard the node from the path
5. End While
6. Establish a new routing path for transmission.
7. End for
8. End.

Fig. 3 illustrates how ERCRM approach isolates the Type III and Type I selfish nodes participating in the routing path based on the values of E_{est} and *ExRC* respectively. The identified Type I and Type III selfish nodes 1 and 4 in the above scenario are isolated from the routing path.

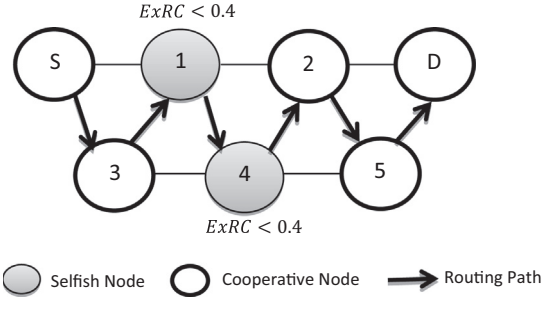

Figure 2 Identification of selfish nodes of Type II based on Exponential Reliability Coefficient (*ExRC*).

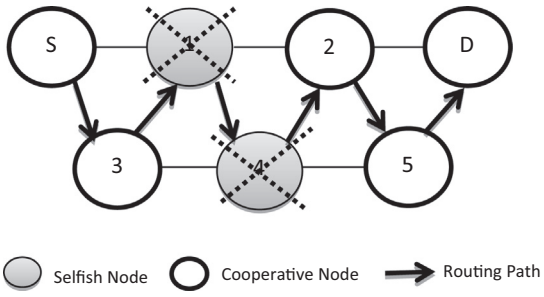

Figure 3 Isolation of selfish nodes from the routing path.

3.5. Correctness of the algorithm

In this section, we prove the correctness of the algorithms which initially detects the presence of selfish nodes based on estimated energy metric and further reconfirms it through the computation of Exponential Reliability Coefficient.

Proposition 1. *Our algorithm 1 proves that any mobile node participating in the routing activity may turn into Type III selfish based on its available energy level*

It has been identified that the implementation of the algorithm 1 in an ad hoc topology (Estimated Energy determination algorithm) estimates the energy level of each and every mobile node based on the residual power and the power drain rate. If the estimated energy level is found to be less than that of the energy required for data transmission, then the node denies forwarding the neighbours' nodes packet in order to conserve its own energy. Hence, it is clear that any mobile node may exhibit Type III selfishness behaviour when it has low energy level.

Proposition 2. *Our algorithm 3 proves that any mobile node participating in the routing activity may turn into Type I selfish node based on its reputation factor*

It has been identified that the implementation of algorithm 3 in an ad hoc topology (Exponential Reliability Coefficient Computational algorithm) computes Exponential Reliability Coefficient (ExRC) for each and every mobile node participating in the routing activity based on second hand information such as packet drop rate and exponential failure rate obtained from the neighbours. If the node has higher value of packet drop rate, then the exponential failure rate of the node gets increases, which in turn reduces the nodes' reliability factor. Hence, it is obvious that the mobile nodes having lower value of Exponential Reliability Coefficient have a greater probability to exhibit type I selfishness behaviour.

4. Simulation experiments and analysis

In this section, in-depth analysis of the characteristics and performance of the proposed ERCRM are studied through simulation using ns 2.26 simulator. The comparative analysis between ERCRM with the existing selfish node mitigation algorithms viz., PCMA, SHRCM and AODV-SELFISHNESS is investigated.

The transmission of data between source and destination highly depends upon the cooperation existing between mobile

nodes present in the routing path [24]. The presence of selfish nodes in the routing path degrades the performance of the network by decreasing the packet delivery ratio. At the same time, it increases the packet drop rate and the number of retransmissions [25]. Hence the performance of the ERCRM is analysed using evaluation parameters viz., packet delivery ratio, throughput, control overhead and total overhead [26,27,7]. The definitions of these parameters are given below.

4.1. Performance metrics

(a) Packet delivery ratio: It is defined as the ratio of the number of data packets delivered to the destination node to the number of data packets generated by the source node.
(b) Throughput: It is defined as the total number of data packets that reach the destination within the total simulation time
(c) Total overhead: It is defined as the sum of the control packets and data packet that is delivered to the destination
(d) Control overhead: It is defined as the total number of bytes of packets that are required for enabling connectivity between the source and destination nodes.

4.2. Simulation configuration

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

4.3. Results and discussions

The performance of the proposed ERCRM is studied based on extensive simulations carried out through four experiments based on the performance metrics proposed in Section 4.1.

In experiment 1, the exponential threshold point of detection is identified, while experiments 2 and 3 are conducted to analyse the performance of ERCRM over PCMA, SHRCM and AODV-SELFISHNESS by varying the number of mobile nodes present in the network with 20% and 40% of mobile nodes as selfish nodes. In addition, experiment 4 is conducted

Table 1 Simulation parameters.

Parameter	Value
Number of mobile nodes	10,20,. . .,100
Protocol used	AODV
Terrain area	1000 m × 1000 m
Mac layer	802.11
Radio range	250 m
Simulation time	100 s
Traffic source	CBR (50 packets/s)
Packet size	512 bytes
Type of antenna	Omni directional antenna
Type of propagation	Two way ground
Channel capacity	2 Mbps
Mobility model	Random way point
Refresh interval time	10 s
Selfish nodes	20% and 40% of the mobile nodes

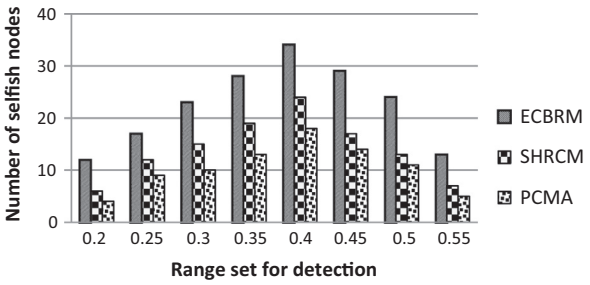

Figure 4 Comparative Chart for ERCRM in Detecting Selfishness.

to evaluate the superior performance of the ERCRM by varying the number of selfish nodes.

4.3.1. Experiment 1 – identification of exponential threshold point of detection

The simulation results of experiment 1 show that the maximum numbers of selfish nodes are identified at the point 0.40 than PCMA and SHRCM. Hence, this point of detection is considered as exponential threshold point. Fig. 4 presents the comparative analysis for identifying the exponential threshold of detection by various mitigation models viz., ERCRM, PCMA and SHRCM.

It is also evident that ERCRM identifies maximum number of selfish nodes in the detection range of 0.35 and 0.45. Therefore, 0.35 and 0.45 are considered as maximum and minimum threshold points for effective selfish node detection.

4.3.2. Experiment 2 – performance analysis of ERCRM by varying the number of mobile nodes (20% of mobile nodes as selfish nodes)

In the simulation experiment 2, the number of mobile nodes is varied from 10 to 100 with 0.4 set as exponential threshold point for detecting selfish nodes. In this experiment, the performance of ERCRM is analysed by considering 20% of the mobile nodes as selfish nodes. Fig. 5(a)–(d) demonstrates the superior performance of ERCRM over PCMA, SHRCM and AODV-SELFISHNESS proposed for mitigating selfish nodes based on packet delivery ratio, throughput, total overhead and control overhead.

Fig. 5(a) presents the performance of ERCRM in terms of packet delivery ratio for varying number of mobile nodes participating in data transmission. It is observed that PDR decreases with increase in the number of mobile nodes cooperating in data transmission. This decrease in PDR is mainly due to the insufficient bandwidth availability since huge amount of data is generated when the number of transmitting nodes increases in an ad hoc environment. However, ERCRM shows an improvement of 8% to 13% in PDR than SHRCM, from 14% to 22% than PCMA and from 19% to 34% than AODV-SELFISHNESS. In addition, ERCRM is an average exhibits a phenomenal improvement of 13% in packet delivery ratio.

Fig. 5(b) shows the performance of ERCRM in terms of throughput for varying number of mobile nodes collaborating during data transmission. It is noticed that, the throughput of the network decreases when the cumulative sum of packets dropped per second by a node increases with increase in number of transmitting nodes. But still, ERCRM increases the

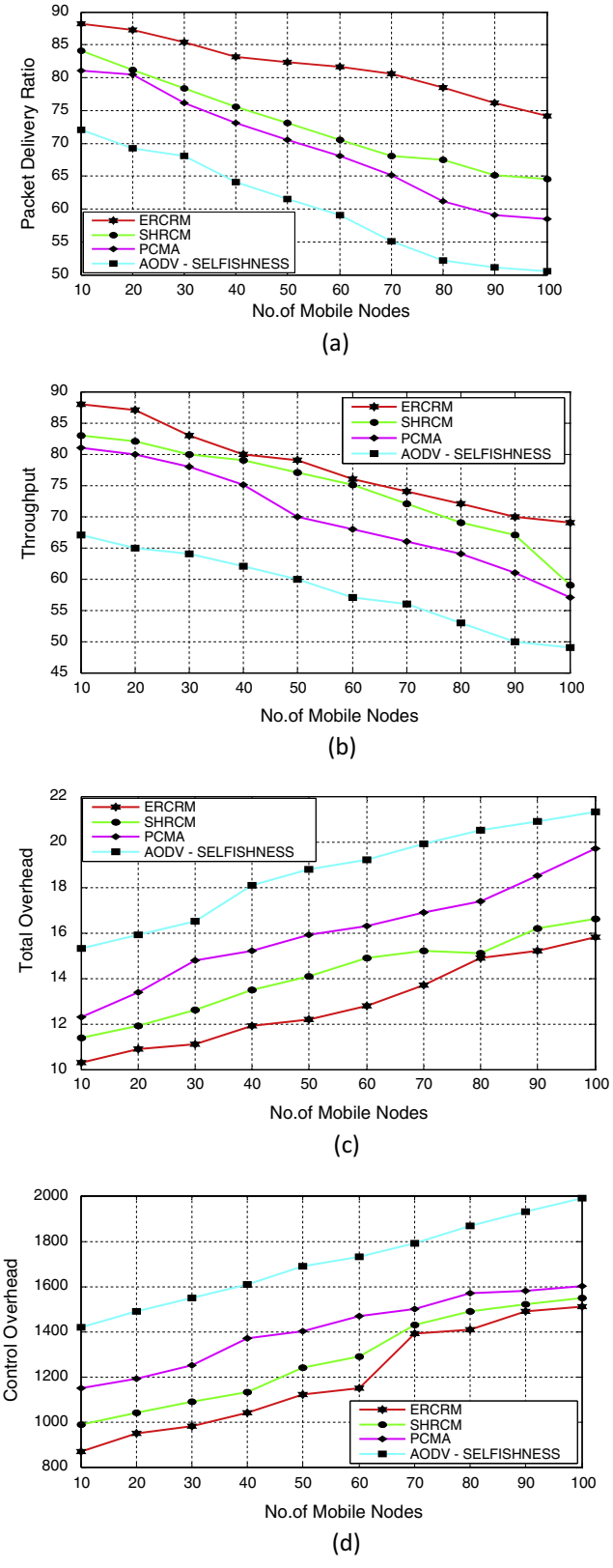

Figure 5 Comparative Analysis of ERCRM approach based on (a) packet delivery ratio (b) throughput (c) total overhead (d) control overhead.

throughput of the network from 7% to 14% than SHRCM, from 14% to 17% than PCMA and from 20% to 27% than AODV-SELFISHNESS mechanisms. Further, it is also evident that ERCRM in an average increases the throughput of the network to the maximum extent of 10%.

Fig. 5(c) and (d) demonstrates the plots for total overhead and control overhead obtained by varying the number of mobile nodes participating in the routing activity. Increase in the number of mobile nodes increases the number of transmission and computations which in turn increases the total overhead and control overhead. But, ERCRM exhibits a decrease of total overhead from 20% to 23% than SHRCM, from 25% to 29% than PCMA and from 31% to 34% than AODV-SELFISHNESS. Similarly, ERCRM also decreases the control overhead from 22% to 27% than SHRCM, from 28% to 34% than PCMA and from 31% to 38% than AODV-SELFISHNESS. In addition, ERCRM in an average reduces the total overhead and control overhead by 11% and 18% respectively.

4.3.3. Experiment 3 – performance analysis of ERCRM by varying the number of mobile nodes (40% of mobile nodes as selfish nodes)

In the simulation experiment 3, the performance of ERCRM is further studied by considering 40% of the mobile nodes as selfish nodes. The Fig. 6(a) –(d) demonstrates the comparative analysis plot of ERCRM with SHRCM, PCMA, AODV-SELFISHNESS mechanisms in terms of packet delivery ratio, throughput, total overhead and control overhead.

ERCRM outperforms SHRCM, PCMA, AODV-SELFISHNESS mechanisms even when the degree of selfishness in the ad hoc environment increases from 20% to 40%. Since, the proposed ERCRM isolates selfish nodes from the routing path at a rapid rate of 28%. Fig. 6 (a) shows that, ERCRM improves the PDR from 6% to 9% than SHRCM, 10% to 16% than PCMA and from 25% to 31% than AODV-SELFISHNESS. Similarly, from Fig. 7(b), it is evident that, ERCRM increases the throughput from 9% to 17% than SHRCM, from 16% to 23% than PCMA and from 26% to 36% than AODV-SELFISHNESS. In addition, ERCRM in an average improves the packet delivery ratio and throughput to a maximum extent of 15% and 18% respectively.

Further, ERCRM substantially, decreases the total overhead and control overhead when compared to SHRCM, PCMA, AODV-SELFISHNESS mechanisms by reducing the number of retransmissions that could occur due to the increase in the number of selfish nodes. Furthermore, from Fig. 6(c), it is evident that ERCRM shows the decrease in total overhead from 24% to 29% than SHRCM, from 28% to 33% than PCMA and from 32% to 37% than AODV SELFISHNESS. Likewise, ERCRM also reduces the control overhead 9% to 13% than SHRCM, 13% to 21% than PCMA and from 28% to 32% than AODV-SELFISHNESS. In addition, ERCRM in an average reduces the total overhead and control overhead at an average rate of 17% and 13% respectively.

4.3.4. Experiment 4 – performance analysis of ECBRM by varying the number of selfish nodes

In simulation experiment 4, the performance of ERCRM is further investigated by varying the number of selfish nodes existing in the ad hoc environment with exponential threshold point for detection as 0.4.

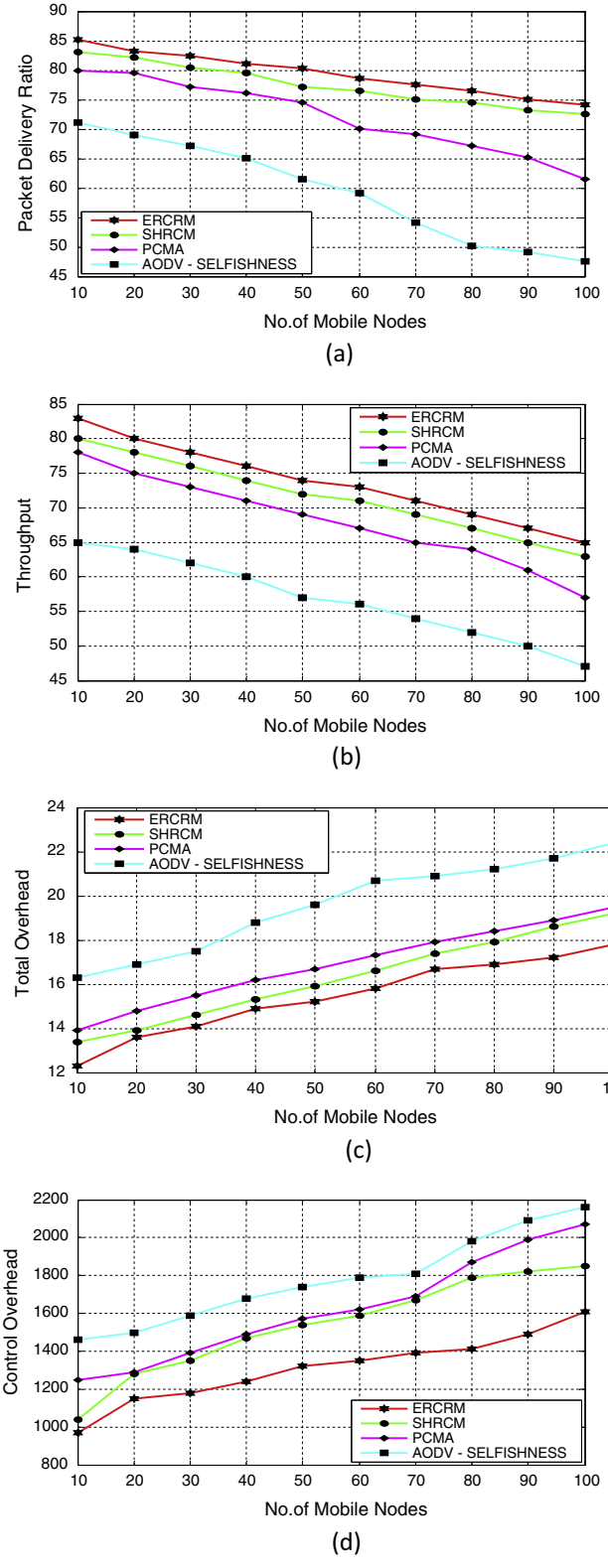

Figure 6 Comparative Analysis of ERCRM approach based on (a) packet delivery ratio (b) throughput (c) total overhead (d) control overhead.

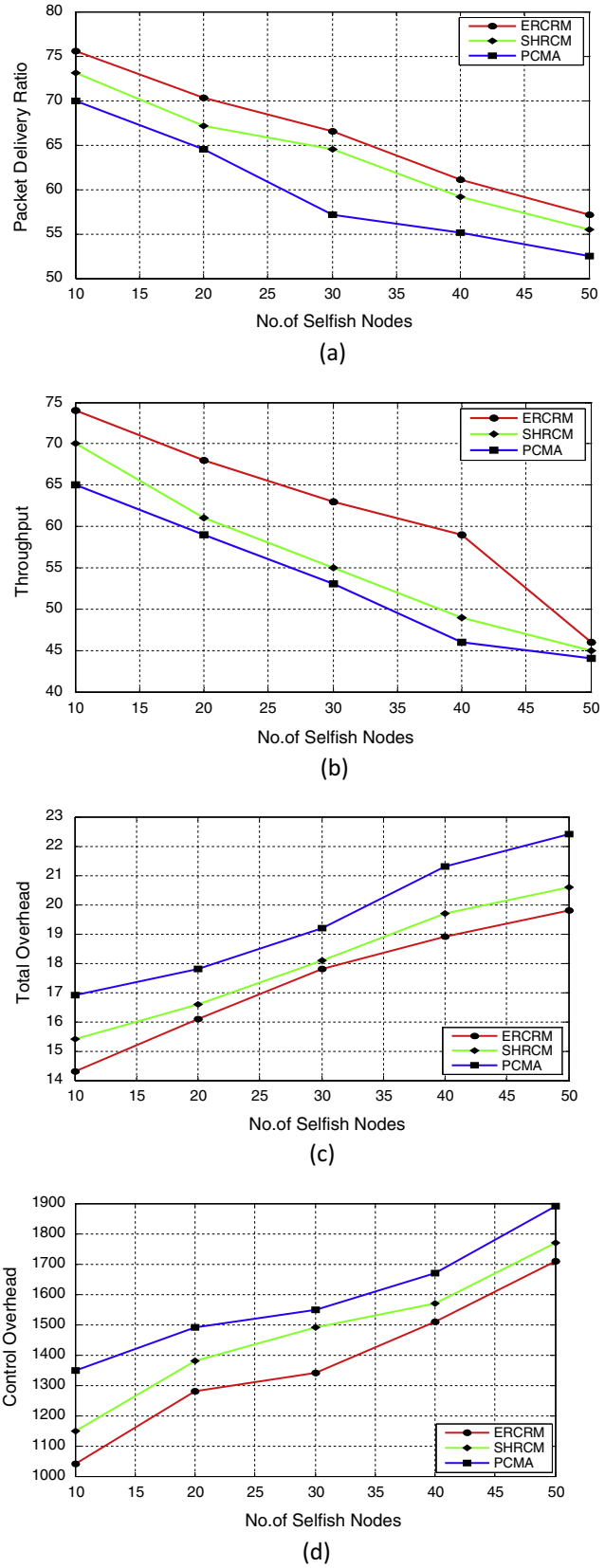

Figure 7 Comparative Analysis of ERCRM approach based on (a) packet delivery ratio (b) throughput(c) total overhead (d) control overhead.

Fig. 7(a) and (b) shows that ERCRM improves the PDR and throughput when compared to SHRCM and PCMA, since SHRCM and PCMA isolate the selfish nodes at a lower rate of 12% and 17% respectively. Further, ERCRM approach increases the packet delivery ratio from 11% to 14% than SHRCM and from 21% to 28% than PCMA. Similarly, ERCRM increases the throughput from 14% to 18% than SHRCM and from 19% to 25% than PCMA. In addition, it is transparent that, ERCRM improves the PDR and throughput at an average rate of 13% and 16% respectively.

Furthermore, from Fig. 7(c) and (d), it is evident that the proposed ERCRM approach decreases the total overhead from 23% to 28% than SHRCM and from 27% to 32% than PCMA and it also decreases control overhead from 21% to 27% than SHRCM and from 24% to 31% PCMA. In addition to this, ERCRM reduces the total overhead and control overhead at an average rate of 16% and 19% respectively.

Finally, the proposed ERCRM approach is further investigated by varying the exponential threshold point set for detection with the minimum and maximum value of 0.35 and 0.45 respectively. At the exponential threshold point 0.35, ERCRM improves the network performance by increasing the packet delivery ratio and throughput at an average rate of 19% and 17% respectively and at the same time decreasing the total overhead and control overhead by 25% and 28.9% respectively. However, at exponential threshold point of 0.45, ERCRM shows only minor improvement in network performance in terms of packet delivery ratio and throughput are 15% and 12% respectively. Similarly it improves the network performance by reducing the total overhead and control overhead by 20% and 23.4% respectively. Hence, the proposed ERCRM approach exhibits optimal performance only when the threshold point of detection is 0.40.

4.4. Major Contributions of ERCRM approach

The major contributions of the proposed Exponential Reliability Coefficient based Reputation Mechanism are summarized as follows.

(a) ERCRM approach aids in defining an exponential threshold point for detection as 0.4, as the simulation result predicts that maximum numbers of selfish node are identified at this point.
(b) From the experimental analysis, it is also clear that the ERCRM mechanism has a successful rate of 28% in isolating the selfish nodes.
(c) Further, the simulation study also makes it clear that the proposed ERCRM approach improves the overall performance of the network in an average rate of 22% when compared to the existing PCMA and SHRCM models.

5. Conclusion

In this paper, we have presented an exponential distribution based cooperation stimulation approach called Exponential Reliability Coefficient based Reputation Mechanism (ERCRM) for mitigating selfish nodes by considering the energy and exponential failure rate into account. Further, the moving average method has been incorporated in our approach for quantifying the reputation level of the mobile nodes through which the decision of isolation is done for enforcing cooperation. The simulation results obtained confirm that the ERCRM outperforms the PCMA and SHRCM in terms of packet delivery ratio, throughput, total overhead and control overhead. Besides, ERCRM also aids in determining 0.40 as the exponential threshold point for detection. The results obtained further confirm that ERCRM in an average improves the packet delivery ratio and throughput by 14% and 17% respectively and at the same time ERCRM reduces the total overhead and control overhead by 19% and 23% when compared to the existing selfish mitigation approaches such as SHRCM and PCMA. Furthermore, it is also evident that the performance of ERCRM is optimal at the minimum (0.35) and maximum (0.45) exponential threshold point of selfish node detection. As a part of the future work, we are planning to devise a reputation based mitigation mechanisms that incorporate kappa and cronbach's statistical coefficient for identifying selfishness behaviour of mobile nodes.

References

[1] Amir Khusru Akhtar, Sahoo G. Mathematical model for the detection of selfish nodes in MANETs. Int J Comput Sci Inform 2009;1(3):25–8.
[2] Bo Wang, Sohraab Soltani, Jonathan Shapiro K, Pang – Ning Tan. Local detection of selfish routing behaviour in ad hoc networks. In: Proc., 8th IEEE international conference on parallel architectures, algorithms and networks, Vol. 1, No. 1; 2005. p. 16–22.
[3] Chen TM, Varatharajan V. Dempster–Shafer theory for intrusion detection in ad hoc networks. IEEE Internet Computing 2009;3(1):234–41.
[4] Pusphalatha M, Revathy V, Rama Rao P. Trust based energy aware reliable reactive protocol in mobile ad hoc networks. World Acad Sci, Eng Technol 2009;3(27):335–8.
[5] Marti S, Gulli TJ, Lai K, Baker M. Mitigating routing misbehaviour 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; 2000. p. 255–65.
[6] Michiardi P, Molva R. 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; 2002. p. 107–21.
[7] Buchegger S, Boudec J-Y. 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; 2002. p. 226–36.
[8] Wang Weizhao, Li Xiang-Yang. Low-cost routing in selfish and rational wireless ad hoc networks. IEEE Trans Mobile Comput 2006;5(5):596–607.
[9] Buttyan L, Hubaux J-P. Stimulating cooperation in self–organizing mobile ad hoc networks. MONET J Mobile Comput Netw 2003;8(1):579–92.
[10] Kargl F, Klenk A, Schlott S, Weber M. 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; 2004. p. 255–63.
[11] Fahad Tarag, Askwith Robert. 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; 2006. p. 78–84.

[12] Zouridaki C, Mark BL, Hejmo M, Thomas RK. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In: Proceedings of the 3rd ACM Workshop on security of ad hoc and sensor networks, vol. 1, no.1; 2009. p. 1–10.

[13] Rizvi S, Elleithy M. A new scheme for minimizing malicious behavior of mobile nodes in mobile ad hoc networks. Int J comput Sci Inform Secur 2009;3(1):25–34.

[14] Komali Ramakant S, MacKenzie Allen B, Gilles Robert P. Effect of selfish node behavior on efficient topology design. IEEE Trans Mobile Comput 2008;7(9):1057–70.

[15] Binglai Niu H, Zhao Vicky, Jiang Hai. A cooperation stimulation strategy in wireless multicast networks. IEEE Transactions on Signal Processing 2011;59(5):2355–69.

[16] Hernandez-Orallo, Manuel D, Serraty Juan-Carlos Cano, Calafate T, Manzoni's. Improving Selfish Node Detection in MANETs Using a collaborative Watchdog. In: IEEE Communication Letters, Vol. 16, No. 5; 2012. p.

[17] Paul K, Westhoff D. Context aware detection of selfish nodes in DSR based ad hoc networks. In: proc., IEEE Globecom, vol. 1, no. 1; 2002. p. 456–62.

[18] Hongxun Liu, Jose G, Delgado-Frias, Srisha Meddi. 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; 2007. p. 179–84.

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

[20] Dehnie Sintanyehu, Tomasin Stefano. Detection of selfish nodes in networks using CoopMAC protocol with ARQ. IEEE Transactions on Wireless Communications 2010;9(7):2328–37.

[21] Sengathir J, Manoharan R. A split half reliability coefficient based mathematical model for mitigating selfish in MANETs. In: Proc., 3rd IEEE International Advance Computing Conference, Ghaziabad, India, vol. 1, no. 1; 2013. p. 267–72.

[22] Annapourna P Patil, Kanth Rajani, Sharanya Bathey, Dinesh Kumar MP, Malavika J. Design of energy efficient routing protocols for MANETs. Int J Comput Sci Issues 2011;8(1):215–20.

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

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

[25] Wu Yanwei, Tang Shaojie, Xu Ping, Li Xiang –Yang. Dealing with selfishness and moral hazard in non-cooperative wireless networks. IEEE Trans Mobile Comput 2010;9(3):420–34.

[26] Khamayseh Yaser, Obiedat Ghadeer, Yassin Munner Bani. Mobility and load aware routing protocol for ad hoc networks. J King Saud Univ –Comput Inform Sci 2011;23(1):105–13.

[27] Amir Khusru Akhtar Md, Sahoo G. Classification of selfish and regular nodes based on reputation values in MANET using adaptive decision boundary. Sci Res J Commun Netw 2013;5(1):185–91.