SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 13, No. 2, June 2016, 265-284

UDC: 519.226:004.421.2 **DOI: 10.2298/SJEE1602265J**

An Erlang Factor-Based Conditional Reliability Mechanism for Enforcing Co-operation in MANETs

Sengathir Janakiraman[1], Manoharan Rajendiran[2]

Abstract: Reputation is considered to be one of the vital entities for maintaining collaboration among wireless mobile nodes present in an ad hoc environment. The nodes in MANET are dynamic and could change its behaviour drastically, but establishing maximum level of cooperation between these nodes is highly crucial. Moreover, the presence of selfish nodes has a greater impact on the resilience of the network. Hence, a need arises for formulating a mechanism that deals with these selfish nodes. In this paper, we contribute an Erlang distribution based Conditional Reliability Mechanism (ECRCM) that aids in detecting and isolating the selfish nodes present in an ad hoc environment. This mathematical model makes the routing decision with the help of a parameter called Erlang factor based Conditional Reliability Coefficient (ECRC) determined for each and every mobile node present in the ad hoc network. Extensive simulations were carried out through ns-2 simulator and the analysis was based on performance metrics such as packet delivery ratio, throughput, control overhead and total overhead. ECRCM also helps in framing an optimal threshold range for selfish node detection. From the results, it is obvious that the threshold range derived in our study remarkably identifies maximum number of selfish nodes when compared to the selfishness detecting parameters available in the literature.

Keywords: Erlang based Conditional Reliability Coefficient, Selfish nodes, Probability of genuineness, Network Resilience, Optimal threshold range, Exponential distribution.

1 Introduction

In MANETs, high degree of collaboration between mobile nodes become vital for enabling efficient rate of data dissemination from the source node to the destination nodes [1]. Since, the mobile nodes in MANETs are connected without any centralized infrastructure; establishing collaboration between these nodes is critical [2]. Numerous mechanisms for detecting misbehaving nodes present in the literature have been formulated mainly based on the assumption that these nodes exploit the network operation without considering its own gain [3]. But, there is a class of misbehaving nodes called selfish nodes, which

[1]Pondicherry Engineering College; E-mails: dr.sengathir@gmail.com, rmanoharan@gmail.com

makes the most use of network resources for their own gain. This kind of exploitation on the network resources by these nodes may result in performance degradation of the entire network [4]. It is also clear that increasing number of selfish nodes may perhaps affect the resilience of the network [5]. Hence, we conclude that there is a need for a mechanism which periodically monitors the presence of selfish nodes in an ad hoc scenario and could take necessary decisions for optimal routing by isolating these nodes.

In this paper, we propose a mathematical model called Erlang distribution based conditional reliability coefficient model for detecting and mitigating selfish nodes. This mathematical model estimates the impact of selfish nodes on the resilience of the network though the conditional reliability coefficient determined based on second hand reputation mechanism. It also estimates the resilience of the network based on two independent exponential parameters viz., a parameter for determining the failure rate of selfish nodes and the other parameter for identifying the failure rate of the network based upon the number of selfish and cooperative nodes present in an existing ad hoc environment. This model is studied based on AODV protocol, which makes control packets viz., RREQ (Route Request), RREP (Route Reply), RERR (Route error) for its connection establishment.

The remaining part of the paper is organized as follows. A brief survey on the related works available in the literature is presented in Section 2. Section 3 depicts the Erlang distribution based Conditional Reliability Coefficient model for isolating selfish nodes. The algorithm used in the deployment of the proposed mathematical model in an ad hoc environment is portrayed in Section 4. Section 5 presents the illustration of the proposed model. The evaluation parameters setup for study and the experimental analysis are enumerated in Section 6 and 7 respectively. Section 8 presents the major contributions of ECRCM and Section 9 concludes the paper.

2 Literature Review

Vast numbers of probabilistic approaches for detecting misbehaving nodes were proposed in the literature from the past decades. Some of those approaches were discussed below.

Initially, a competent Bayesian approach proposed by S.Buchegger and J.L Boudec[6] was formulated mainly for estimating the level of reputation possessed by each and every nodes present in an ad hoc scenario. The reputation rating for the individual nodes is calculated based on Beta distribution, which is an adaptive version of Bernoulli distribution. The nodes in the network are generally classified as normal or misbehaving node based on the threshold tolerance. They considered prior probability as (1, 1) and event modeled as uniform distribution on between (0, 1). This first hand reputation mechanism

also addressed various vulnerabilities that could originate due to the decrease in the reputation level. The main advantage of this system lies in its capacity of discriminating selfish nodes from co-operative nodes but the detection rate facilitated by them is minimal. Another probabilistic based tamper resistant model that uses a tamper resistant hardware was proposed by Buttyan and Hubaux [7] for isolating the malicious behaviour of nodes. The core concept behind this detection is the Nuglet counter. This counter monotonically increases or decreases based on the role of the node as a sender or router. This mechanism has established a high degree of trust by enhancing cooperation through the incorporation of nuglet counter in self-organizing mobile ad hoc networks but the degree of discrimination between partial and complete selfish behaviour is not well defined.

Further, an evidence model which works based on conditional probability was proposed by Kargl et al., 8]. In this model, the routing decisions were based on the negotiation among the mobile nodes existing in the network. This evidence model is capable of over hearing a routing protocol. The protocol used in this study is SDSR and the detection mechanisms are deployed in a secured architecture called SAM. But, SDSR is not capable of collecting complete evidence. In another evidence based approach was introduced by Thomas M.Chen and Varatharajan Venkataraman [9]. They introduce an evidence theory that estimates the degree of cooperation existing between the nodes in the network during uncertainty. They also formulated a numerical procedure called Dempster rule of combination which combines multiple evidences into a hybrid rule. This numerical procedure was based on the evidences collected from the neighbour nodes. In addition, this posterior probability method uses two thresholds viz., belief and plausibility. A probabilistic detection framework based on opinion metric was proposed by C. Zouridzki et al. [10]. An opinion metric was formulated by considering the first and second information collected from the routers of the network. Statistical trust and confidence values were also used for confirming the reliability in delivery of packets in the network. This mechanism suffers from the criticism that trust and confidence obtained through statistical means may not be the optimal way of computing genuineness behaviour in mobile nodes.

Furthermore, an efficient monitoring algorithm called Packet Conservation Monitoring Algorithm has been proposed by Tarag Fahad and Robert Askwith [11]. This algorithm deals with the selfish nodes based on the neighbouring nodes that has sent or received dual information either from or to the misbehaving node. This mechanism conserves energy to the maximum. The authors proposed this mechanism to detect the special case of selfish nodes that drops the packets partially based on degree of trust. Hernandez-Orallo et al. [12] contributed a component based mathematical detection model that makes it decision based on watchdog mechanism. The occurrences of communication

between any two mobile nodes in this model are assumed to follow Poisson distribution. The authors used two states viz., NOINFO and POSITIVE for detecting the selfishness of nodes. The modeling of the network was based on continuous state Markov chain expressed with the aid of transition probability matrix with canonical form. Senthilkumar et al. [13] proposed a Record-and Trust-Based Detection (RTBD) mechanism for detecting selfish nodes by using trust in order to accelerate the rate of detection. RTBD investigates the detection of selfish nodes by verifying the vital network functionalities that corresponds to packet dropping and routing characteristics of participating mobile nodes. RTBD also exhibits a phenomenal improvement in terms of decreased detection time and total overhead. Jebakumar et al. [14] proposed a token-based umpiring technique (TBUT) in which an individual nodes necessitates a token for participating in the network activities. In TBUT, the neighbouring nodes of each mobile node carry out the act of umpire and it incurs less overhead and minimized detection time. It is proved that TBUT is predominant in enhancing the network performance and improving the security of most of the real applications. Smitha et al. [15] proposed a selfish node detection algorithm called SIAODV for quantifying the degree of risk incurred for estimating the optimum path incurred in packet forwarding. SIAODV focuses only on the minimum risk path in packet dissemination rather than shortest path of routing which is predominantly used in most of the existing mitigation approaches.

In addition, Yu et al. [16] contributed a service-based selfish routing protocol named SSR for making decisions on effective forwarding. SSR is based on the concept of user altruism that is determined based on two perspectives that highlights individual and social node's selfishness. This altruistic approach employs two services like social and pair-wise services as incentives for enforcing co-operation between the mobile nodes. In SSR, the nodes that favours high degree of altruism is chosen as the relay node but the concept of altruism cannot be considered as the reliable parameter for decision making. Hernendez-orallo [17] contributed a collaborative contact-based watchdog (CoCoWa) that uses the concept of diffusion of selfish nodes based on a local repair technique. This CoCoWa mechanism is more advantageous than the traditional watchdog since they may reduce the performance of the network in terms of speed and precision. Moreover, the false positive and false negative rate of classical watchdog is comparatively greater than CoCoWa as they incorporate a situational awareness of selfishness when neighbouring mobile nodes come into contact. CoCoWa greatly reduces the cost of transmission by accurately predicting the selfish behaviour of nodes. Authors of this paper also has proposed a Reliability Factor Based Mitigation Mechanism (RFBMM) [18] that estimates the reliability of the mobile nodes through a packet deficiency parameter. This reliability parameter is computed based on the weighted sum of product of the estimated normalized deficiency factor

which has been collected for some session period. The isolation of the selfish nodes in RFBMM is achieved only through the exponential function of normalized deficiency factor that portrays its availability in routing. This mechanism does not consider first hand reputation of mobile node into consideration and rather relies only on past history.

Extract of the Literature

The conditional probabilistic approaches for detecting and isolating selfish nodes present in the literature have the following shortcomings. They are

i) An Erlang based conditional probabilistic approach for detecting and mitigating selfish node behaviour has not been proposed to the best of our knowledge.

ii) A mechanism that makes the routing decision in the presence of selfish nodes considering the resilience of individual nodes as well as the entire network at any instant has not been explored.

Hence, the limitations of the available conditional probabilistic approaches have motivated us for innovating a mechanism for detecting selfish nodes based on Erlang distribution.

3 Erlang Based Conditional Reliability Co-Efficient Model (ECRCM)

In this section, we contribute a mathematical model called Erlang based Conditional Reliability Co-efficient Model. This mathematical model aids in the detection of selfish nodes based on a factor called Erlang based Conditional Reliability Co-efficient, which is manipulated for identifying the impact level of selfish nodes on the resilience of the network. This conditional probabilistic approach not only identifies the reliability of individual nodes but also aids in determining the resilience of the network.

Let us consider an ad hoc environment containing both selfish nodes (non-cooperative nodes) and non-selfish nodes (co-operative nodes) and ‘x’ be the estimated life time of the network.

The probability for a node to become selfish within the network lifetime time ‘*x*’ is given by (1),

$$a = \frac{No \cdot ofpacketsforwardedforitsneighbours}{No \cdot ofpacketsreceivedfromtheirneighbours}, \tag{1}$$

where ‘a’ is the probability of genuineness identified for a node.

Let ‘*y*’ be considered as a random variable used for classifying the nodes in ad hoc scenario as selfish and co-operative based on the value of ‘a’. If the value of ‘*a*’ reaches below the threshold value of 0.50 as proposed in [1], then

the particular node may be called as selfish. But when the value of 'a' is above the threshold, and then the node is said to exhibit normal behaviour.

If a node is with probability (1–*a*) then it is said to be in normal behaviour. At the same time, the node possesses selfish behaviour with the probability a, given by (2) and (3),

$$P_y(0) = 1 - a\,, \tag{2}$$

$$P_y(1) = a\,. \tag{3}$$

Thus, the random variable '*y*' is defined as below,

y = 0, if a node exhibits normal behaviour;

y = 1, If a node exhibits selfish behaviour

Let us assume the network consists of '*n*' nodes, in which there are '*m*' co-operative nodes and (*m*–*n*) selfish nodes. Then, the probability for a node to exhibit normal behaviour 'λ' is given by (4) and (5),

$$\lambda = \frac{m}{n}(1-a) + \frac{m-n}{n}a\,. \tag{4}$$

Under the condition,

i) '*m* out of *n*' nodes are co-operative with probability (1–*a*) and

ii) (*m*–*n*) out of *n* nodes are selfish with probability '*a*'.

Thus,

$$\lambda = \frac{m - na}{n}\,. \tag{5}$$

Since, the network lifetime '*x*' could be expressed as the sum of two independent exponentially distributed random variables, each of parameter λ.

Thus, the failure rate of co-operative nodes in any time't' is given by (6),

$$f_{x/y}(y=0) = \lambda\, \mathrm{e}^{-\lambda t}\,. \tag{6}$$

In contrast, the failure rate of selfish nodes in any time '*t*' are Erlang distributed, which is given by (7),

$$f_{x/y}(y=1) = \lambda^2 t\, \mathrm{e}^{-\lambda t}\,. \tag{7}$$

Since, Erlang distribution is a kind of phase type distribution which depends upon sum of independent exponential random variables. This distribution is considered for identifying the failure rate network.

In this scenario, the failure rate of entire network depends on the failure rate of co-operative nodes as well as selfish nodes with probability of (1–*a*) and (*a*) respectively. Hence, the failure rate of entire network is given by (8),

$$f_{x/y}(y=0)+f_{x/y}(y=1)=\lambda(1-a)\mathrm{e}^{-\lambda t}+\lambda^2 at\,\mathrm{e}^{-\lambda t}. \quad (8)$$

Thus, the Erlang based Conditional Reliability Coefficient (ECRC) for identifying the impact level of selfish nodes on the network at any time '*t*' is given by (9)

$$R_{x/y}(t)=(1+a\lambda t)\mathrm{e}^{-\lambda t}. \quad (9)$$

In general, the level of impact of selfish nodes on the resilience of the network could be identified based on the values of ECRC. If the ECRC value is nearer to zero, then the impact of selfishness is less. In contrast, when the ECRC value diverges from zero, then the impact of selfishness increases significantly. This Erlang based Conditional Reliability Coefficient Model also aids in framing an optimal range for detecting selfish nodes. The proposed mechanism is a distributed model deployed in each and every mobile node of the ad hoc environment.

4 Algorithms for Erlang Based Conditional Reliability Coefficient Model

The proposed Erlang based Conditional Reliability Coefficient Model can be implemented using two algorithms viz., algorithm 1 (Pseudo code for detecting selfish nodes based on probability of genuineness) and algorithm 2 (Pseudo code for identifying the impact of selfishness on network resilience).

Algorithm 1 details on the procedure detection( ) identifies the node's selfishness based on the value of 'a', which is called as the probability of genuineness for a node. Every node in the ad hoc environment is monitored for its behaviour and if the value of 'a' is less than 0.30 as derived from (1), then the node is set to a random variable *y*=1. Else, the node is set to be in normal behaviour with random variable *y*=0. With the help of random variable 'y', the number of normal and selfish nodes in the scenario is identified.

Algorithm 2 determines the network resilience based on the impact of selfishness. The procedure resilience( ) initially, computes the probability of normal behaviour 'λ' using (5), with the aid of parameters viz., number of normal nodes and number of selfish nodes computed in the algorithm 1. As a next step, the ECRC value for the entire network using 'λ' is computed based on (8), which is obtained by the cumulative sum of failure rates for selfish behaviour based on (7) and the failure rate of normal nodes based on (6). When the ECRC value for the network is above the threshold of resilience (0.4), then the selfish node in the routing path is isolated using isolate( ) procedure. As per the simulation conducted in this paper, the threshold value is obtained as 0.4. This value is considered to be the threshold of resilience, since the simulation results shows a phenomenal increase in the packet delivery ratio and throughput with this value.

Algorithm 1: Pseudo code for detecting selfish nodes based on probability of genuineness

Notations:

n- Indicates the total number of nodes in the network

N_i – Indicates each and every node in the ad scenario, where $0 < i < n$.

1: detection () Begin
2: for (each mobile node in the network N_i) Begin
3: Compute probability of genuineness 'a' using (1).
4: if $(a < 0.30)$ *then;*
5: Set $y = 1$ *and mark it as selfish node*
6: else Set $y = 0$ *and mark it as normal node;*
7: End if.
8: End for
9: for (all n mobile nodes in the network) Begin
10: if (the values for node $(N_i(y) == 0)$*)*
11: then $m = m + 1$*; /*counts the number of cooperative nodes*/*
12: End if
13: End for
14: $k = n - m$ */*count for selfish nodes*/*

Algorithm 2: Pseudo code for identifying the impact of selfishness on network resilience

/ when m and k are determined */*

1: resilience () Begin
2: for (each mobile node Ni) Begin
3: Manipulate the probability of normal behaviour 'λ' with (5);
4: End for
5: for (each selfish node in the network N_i) Begin
6: If $(N_i(y) == 1)$
7: Compute failure rate using Erlang distribution based on the value 'λ' with (7);
8: Else
9. Compute failure rate of normal nodes with (6)
10: End if
11: End for
12: Compute ECRC with the aid of (8) using the failure rates obtained from (6) and (7)
13: If (ECRC is greater than threshold of resilience)
14: Call isolate ();
15: Else
16: Normal Routing.
17: End if.
18: End

6 Simulation Setup

An extensive simulation for the proposed model was carried through network simulator ns-2.26. In the ad hoc environment, 100 mobile nodes are deployed in the terrain size of 1,000 X 1,000. The channel capacity and refresh internal time for the simulation run are 2 Mbps and 10 seconds respectively. The following **Table 1** represents the simulation parameter setup for study.

Table 1
Simulation Setup.

Parameter Name	Value
Number of Nodes	100
Protocol used	AODV
Mac Layer	802.11
Terrain area	1000X1000 Sq. meters
Simulation Time	100 seconds
Traffic model	Constant bit rate
Packet size	512 bytes
Type of antenna	Antenna/Omni antenna
Type of Propagation	Two ray ground

6.1 Evaluation Parameters

The presence of selfish nodes in the network decreases packet delivery ratio and throughput, while it increases the total overhead and control overhead in ad hoc scenario [19-21]. Hence the proposed ECRCM scheme is analysed based on the metrics enumerated below.

i) Packet delivery ratio*:* It is defined as the ratio of number of packets received by a node to the total number of packets actually designated for it.

ii) Throughput*:* It is defined as the maximum number of data packets delivered to the destination nodes with time‘t’

iii) Total overhead*:* It is defined as the ratio of number of packets necessary for the route establishment to the number of data packets that reaches the destination.

iv) Control Overhead*:* It is defined as the maximum size of the packets that are utilized for establishing the connection between the source node and destination node.

7 Experimental Results and Analysis

The experimental result makes it obvious that maximum numbers of selfish nodes are identified, when the threshold point set is set i.e., 0.30. Fig. 1 interprets the possible number of selfish nodes that could be identified using different set of values for detection.

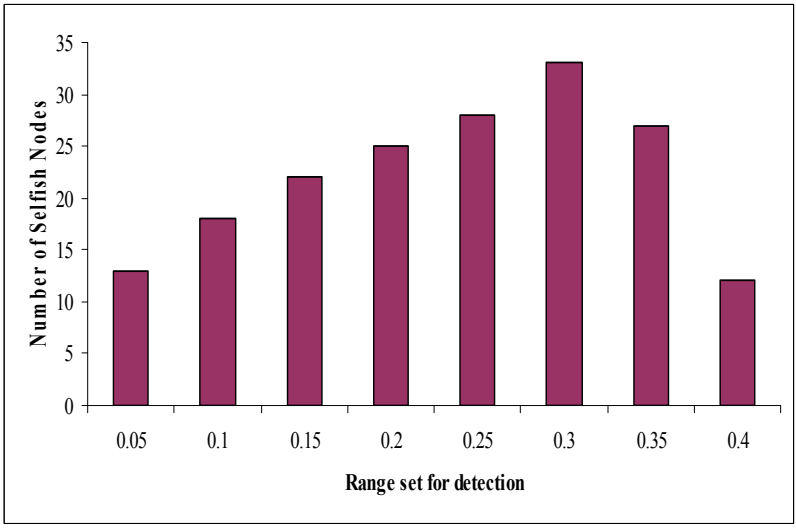

Fig. 1 – *Chart representing the range set for identifying selfish nodes using ECRCM.*

Since, maximum numbers of selfish nodes are identified in the threshold range i.e., 0.35 to 0.25, they are considered to be the Minimum and Maximum threshold for detection respectively.

7.1 Performance analysis for ECRCM based on number of mobile nodes

In this experiment, the performance of the network is evaluated in terms of packet delivery ratio, throughput, control overhead and total overhead obtained by varying the number of mobile nodes. Figs. 2 and 3 depicts the performance of the network based on packet delivery ratio and throughput compared with four schemes, viz., without selfishness, with selfishness, with PCMA and with ECRCM. The results predict that packet delivery ratio and throughput decreases exponentially when the number of mobile nodes present in an ad hoc scenario increases. It is evident that ECRCM is phenomenal in sustaining the packet delivery rate and throughput than PCMA, since it considers path stability and node stability for selfish node mitigation.

The proposed ECRCM scheme increases the packet delivery ratio and throughput to a maximum of 13% and 12% respectively when compared to PCMA.

Further, Figs. 4 and 5 presents the performance of the network based on control overhead and total overhead compared with four schemes, viz., without selfishness, with selfishness, with PCMA and with ECRCM. It is evident that the control overhead and total overhead of the network increases drastically when the number of selfish nodes presents in an ad hoc scenario increases. But ECRCM is potential enough in reducing the control overhead and total

overhead than PCMA as it incorporates an integrated approach that quantifies the impact of both historical and present behaviour into account. Thus ECRCM decreases the control overhead and total overhead to a maximum of 23% and 27% than PCMA.

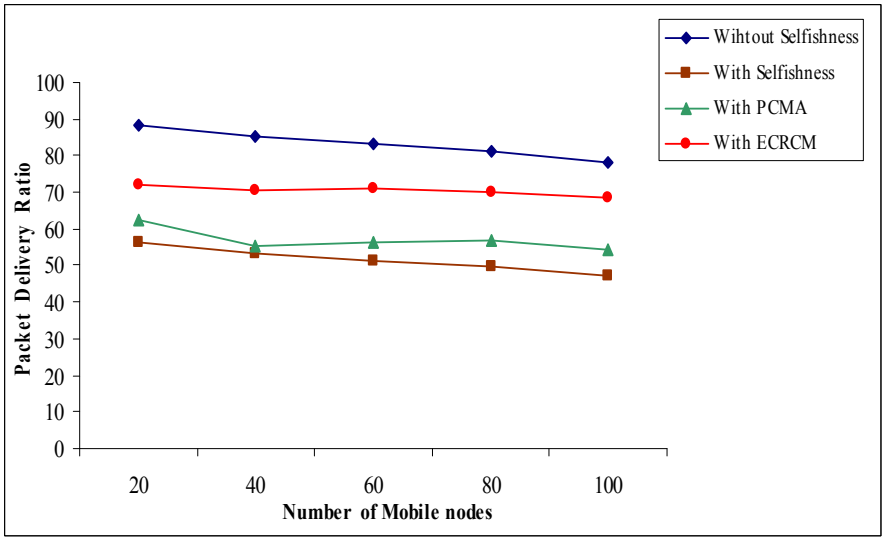

Fig. 2 – *Performance analysis chart for ECRCM based on packet delivery ratio.*

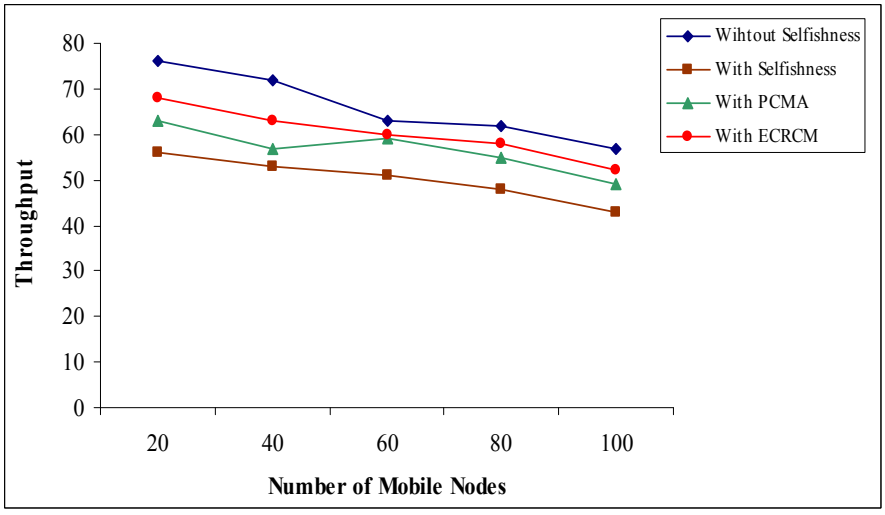

Fig. 3 – *Performance analysis chart for ECRCM based on throughput.*

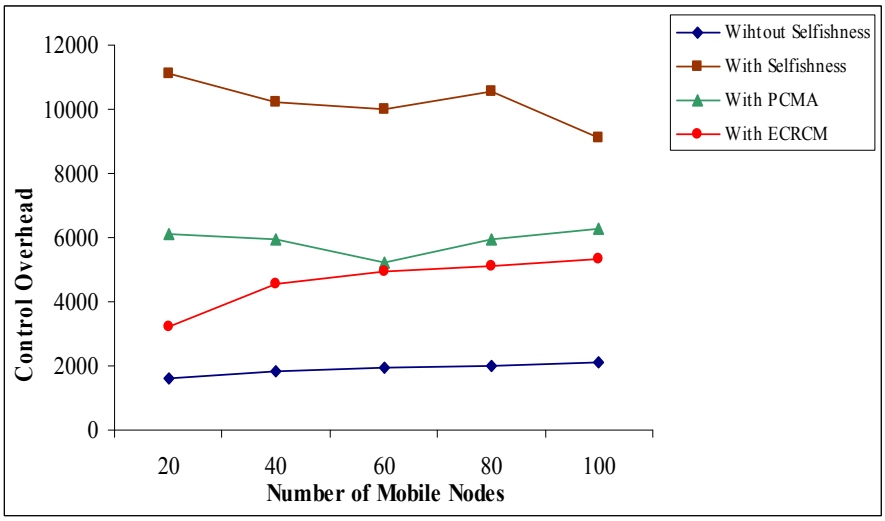

Fig. 4 – *Performance analysis chart for ECRCM based on control overhead.*

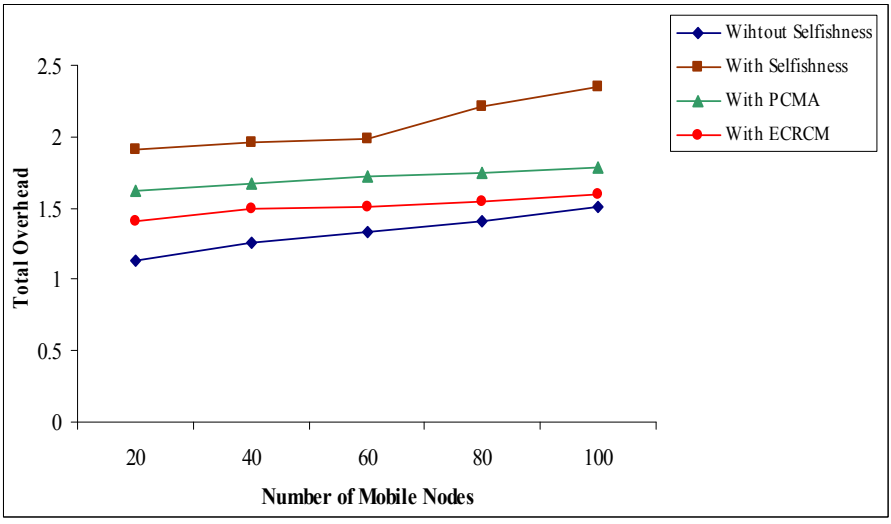

Fig. 5 – *Performance analysis chart for ECRCM based on total overhead.*

7.2 Performance analysis for ECRCM based on maximum and minimum threshold by varying number of mobile nodes

In this experiment, the performance of the network is evaluated in terms of packet delivery ratio, throughput, control overhead and total overhead obtained by varying the number of mobile nodes under the influence of minimum and maximum threshold of detection. Figs. 6 and 7 depicts the performance of the

network based on packet delivery ratio and throughput compared with four schemes, viz., with selfishness, with MIN threshold based detection for ECRCM and with MAX threshold based detection for ECRCM.

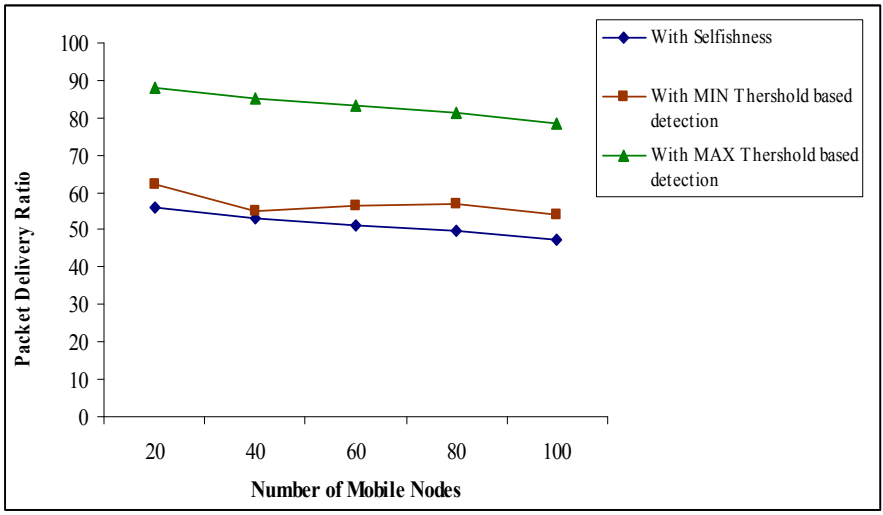

Fig. 6 – *Performance chart for ECRCM (MAX and MIN threshold) based on packet delivery ratio.*

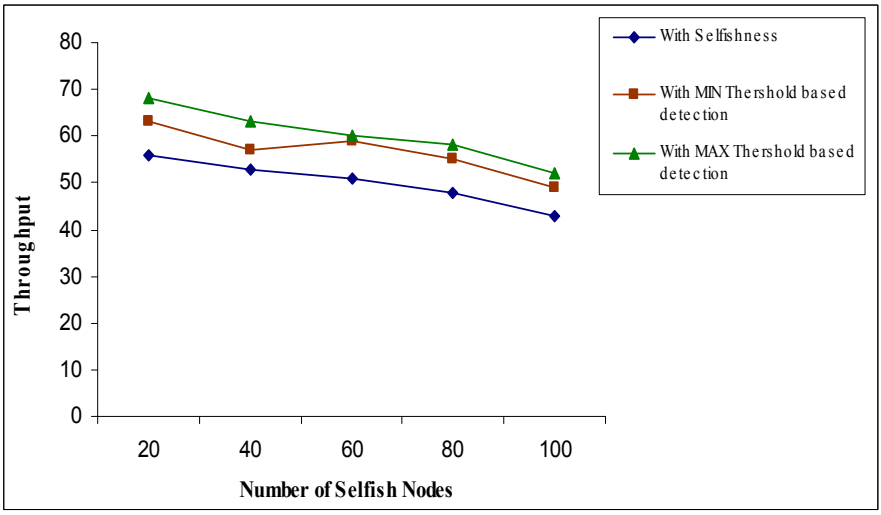

Fig. 7 – *Performance analysis chart for ECRCM (MAX and MIN threshold) based on throughput.*

The results predict that packet delivery ratio and throughput decreases exponentially when the number of mobile nodes present in an ad hoc scenario increases. It is evident that ECRCM is phenomenal in sustaining the packet delivery rate and throughput than PCMA as it considers the integration of both node's packet rate and its participative index into account.

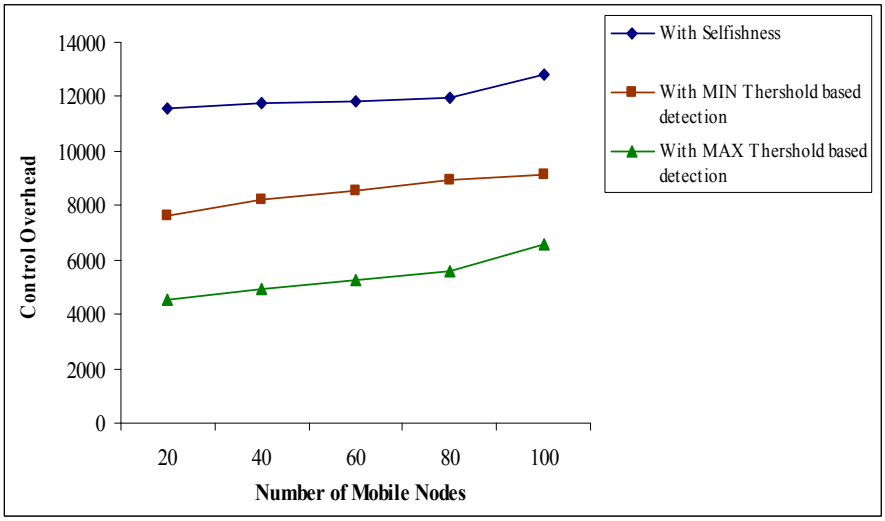

Fig. 8 – *Performance analysis chart for ECRCM based on control overhead.*

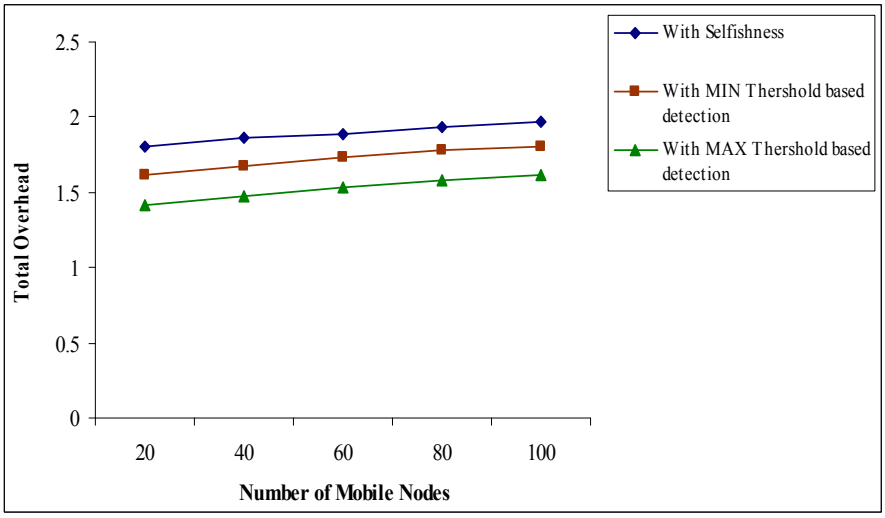

Fig. 9 – *Performance analysis chart for ECRCM (MAX and MIN threshold) based on total overhead.*

Thus, ECRCM when implemented increases the packet delivery ratio to an extent of 11% using minimum threshold based detection, while in case of maximum threshold based detection, it increases up to 25%. Similarly, ECRCM increases the throughput to an extent of 19% using minimum threshold based detection and 31% in case of maximum threshold based detection.

Furthermore, Figs. 8 and 9 represents the performance of the network based on control overhead and total overhead compared with four schemes, viz., with selfishness, with MIN threshold based detection for ECRCM and with MAX threshold based detection for ECRCM. The results prove that control overhead and total overhead is phenomenal reduced by facilitating a rapid detection rate of 28% superior to PCMA.

ECRCM thus reduces control overhead to a maximum of 18% under minimum threshold based detection and 32% in case of maximum threshold based detection. In addition, it decreases total overhead up to a maximum of 13% and 29% under the influence of minimum and maximum threshold based detection.

8 Major Contributions of ECRCM

The major contributions of the proposed Erlang based Conditional Reliability Coefficient Model may be summarized as follows:

a) We define the threshold point of detection as 0.3, as the simulation results infer that maximum numbers of selfish node are identified at this saddle point.

b) We show that the resilience of network depends on the number of selfish nodes present in the environment, i.e., when the ECRC value is below the value of threshold of resilience (0.4) then the impact of selfish node in the network resilience is low. But, when the ECRC value is above 0.4, then the impact of selfish node in the network is high.

c) From the experimental analysis, we are able to devise a minimum and maximum threshold level of detection as 0.35 and 0.25 respectively.

d) We also infer that depending on the decrease in value of λ, the probability of selfishness increases.

In addition, the performance of ECRCM is investigated by varying bigger number of mobile nodes, the type of traffic model utilized and the size of the packet used for transmission, and the results are represented form **Tables 2 – 10**.

Table 2
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on increase in PDR (varying bigger number of mobile nodes).

Number of Mobile nodes	Selfish node Mitigation schemes				
	ECRCM	**RTBD**	**TBUT**	**RFBMM**	**PCMA**
100	17%	15%	11%	9%	7%
150	12%	11%	8%	6%	5%
200	10%	9%	6%	5%	4%

Table 3
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on increase in throughput (varying bigger number of mobile nodes).

Number of Mobile nodes	Selfish node Mitigation schemes				
	ECRCM	**RTBD**	**TBUT**	**RFBMM**	**PCMA**
100	17%	15%	11%	9%	7%
150	12%	11%	8%	6%	5%
200	10%	9%	6%	5%	4%

Table 4
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on decrease in total overhead (varying bigger number of mobile nodes).

Number of Mobile nodes	Selfish node Mitigation schemes				
	ECRCM	**RTBD**	**TBUT**	**RFBMM**	**PCMA**
100	16%	13%	11%	9%	7%
150	14%	11%	10%	8%	6%
200	13%	10%	8%	5%	4%

Table 5
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on increase in PDR (varying mobility models).

Traffic Model	Selfish node Mitigation schemes				
	ECRCM	**RTBD**	**TBUT**	**RFBMM**	**PCMA**
Random waypoint	20%	17%	14%	11%	10%
Random direction	18%	14%	10%	7%	6%
Random walk	16%	15%	13%	9%	8%

Table 6
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on increase in throughput (varying mobility models).

Traffic Model	Selfish node Mitigation schemes				
	ECRCM	RTBD	TBUT	RFBMM	PCMA
Random waypoint	18%	15%	12%	10%	8%
Random direction	14%	13%	10%	8%	6%
Random walk	17%	14%	9%	9%	4%

Table 7
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on decrease in total overhead (varying mobility models).

Traffic Model	Selfish node Mitigation schemes				
	ECRCM	RTBD	TBUT	RFBMM	PCMA
Random waypoint	26%	23%	22%	21%	18%
Random direction	17%	16%	18%	14%	13%
Random walk	21%	18%	15%	19%	16%

Table 8
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on increase in PDR (varying packet size).

Packet size	Selfish node Mitigation schemes				
	ECRCM	RTBD	TBUT	RFBMM	PCMA
256	23%	21%	18%	16%	12%
512	20%	18%	14%	13%	8%
1024	17%	14%	12%	10%	5%

Finally, the performance of ECRCM is also compared with the benchmark selfish node mitigation approaches like RTBD, TBUT and ETUS, and the results are portrayed in **Table 11**.

Table 9
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on increase in throughput (varying packet size).

Packet size	Selfish node Mitigation schemes				
	ECRCM	**RTBD**	**TBUT**	**RFBMM**	**PCMA**
256	21%	17%	15%	13%	10%
512	18%	15%	12%	11%	8%
1024	15%	13%	11%	9%	6%

Table 10
Performance of ECRCM, RTBD, TBUT, RFBMM and PCMA based on decrease in total overhead (varying packet size).

Packet size	Selfish node Mitigation schemes				
	ECRCM	**RTBD**	**TBUT**	**RFBMM**	**PCMA**
256	13%	11%	10%	8%	6%
512	10%	8%	7%	5%	4%
1024	8%	5%	4%	3%	2.5%

Table 11
Mean Performance Evaluation of ECRCM, RTBD, TBUT and RFBMM.

Selfish node Mitigation schemes	Increase in PDR	Increase in throughput	Decrease in control overhead	Decrease in total overhead
ECRCM	21%	23%	22%	31%
RTBD	14%	17%	13%	25%
TBUT	8%	13%	11%	24%
RFBMM	7%	11%	7%	21%
PCMA	5%	8%	6%	14%

9 Conclusion

In this paper, the impact of selfish nodes on the network resilience has been studied based on Erlang based Conditional Reliability Coefficient Model

(ECRCM). The proposed ECRCM detects the maximum number of selfish nodes when compared to the existing PCMA model available in the literature. In an average, the ECRC Model has a successful detection rate of 28%, which is found to be remarkable. The experimental results make it evident that this approach outperforms the PCMA model in terms of packet delivery ratio, throughput, control overhead and total overhead. In addition, this model aids us in framing a value of 0.3, the saddle point for selfish detection and also the threshold of resilience as 0.4.

10 References

[1] A.K. Md. Akhtar, G. Sahoo: Mathematical Model for the Detection of Selfish Nodes in MANETs, International Journal of Computer Science and Informatics, Vol. 1, No. 3, 2008, pp. 25 – 28.

[2] S. Buchegger, J.Y. Boudec: Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad-Hoc Network, 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, 09-11 Jan. 2002, pp. 403 – 410.

[3] S. Marti, T.J. Giuli, K. Lai, M. Baker: Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks, 6th Annual international Conference on Mobile Computing and Networking, Boston, MA, USA, 06 – 11 Aug. 2000, pp. 255 – 265**.**

[4] S.S. Rizvi, K.M. Elleithy: A New Scheme for Minimizing Malicious Behaviour of Mobile Nodes in Mobile Ad Hoc Networks, International Journal of Science and Information Security, Vol. 3, No. 1, July 2009, pp. 45 – 54.

[5] P. Michiardi, R. Molva: CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks, Communication and Multimedia Security, Protoroz, Solvenia, 26-27 Sept. 2002.

[6] S. Buchegger, J.Y. Boudec: Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes – Fairness in Distributed Ad-hoc Networks, 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, Switzerland, 09-11 June 2002, pp. 226 – 236.

[7] L. Buttyan, J.P. Hubaux: Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, Mobile Computing and Networking, Vol. 8, No. 5, Oct. 2003, pp. 579 – 592.

[8] F. Kargl, A. Klenk, S. Schlott, M. Weber: Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks, 1st European Workshop on Security in Ad-Hoc and Sensor Network, Heidelberg, Germany, 06 Aug, 2004, pp. 152 – 165.

[9] T.M. Chen, V. Varatharajan: Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks, IEEE Internet Computing, Vol. 9, No. 6, Nov/Dec. 2005, pp. 35 – 41.

[10] C. Zouridzki, B.L. Mark, M. Hejmo, R.K Thomas: A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs, 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, Virginia, USA, 07 Nov. 2005, Vol. 1, pp. 1 – 10.

[11] T. Fahad, R. Askwith: A Node Misbehaviour Detection Mechanism for Mobile Ad Hoc Networks, 7th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, Liverpool, UK, 26-27 June 2006.

[12] E. Hernandez-Orallo, M.D. Serrat, J-C. Cano, T. Calafate, P. Manzoni: Improving Selfish Node Detection in MANETs using a Collaborative Watchdog, IEEE Communications Letters, Vol. 16, No. 5, May 2012, pp. 642 – 645.

[13] S.K. Subramaniyan, W. Johnson, K. Subramaniyan: A Distributed Framework for Detecting the Selfish Node in MANET using Record and Trust-Based Detection (RTBD) Technique, EURASIP Journal on Wireless Communication and Networking, Vol. 2014, No. 1, Dec. 2014, p. 205.

[14] J.M.S.P.J. Kumar, A. Kathirvel, N. Kirubakaran, P. Sivaraman, M. Subramaniam: A Unified Approach for Detecting and Eliminating Selfish Nodes in MANETs using TBUT, EURASIP Journal on Wireless Communications and Networking, Vol. 2015, No. 1, Dec. 2015, p. 143.

[15] S. Rukhande, P. Shete: Optimized Routing by Excluding Selfish Nodes for MANET, Communications on Applied Electronics, Vol. 3, No. 5, Nov. 2015, pp. 43 – 49.

[16] L. Yu, P. Liu: A Service-Based Selfish Routing for Mobile Social Networks, International Journal of Distributed Sensor Networks, Vol. 2015, 2015, p. 910635.

[17] E. Hernandez-Orallo, M.D. Serrat, J-C. Cano, C.T. Calafate, P. Manzoni: CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes, IEEE Transactions on Mobile Computing, Vol. 14, No. 6, June 2015, pp. 1162 – 1175.

[18] J. Sengathir, R. Manoharan: A Reliability Factor Based Mathematical Model for Isolating Selfishness in MANETs, International Journal of Information and Communication Technology, Vol. 6, No. 3/4, July 2014, pp. 403 – 421.

[19] C.A.V. Campos, L.F.M. de Moraes: A Markovian Model Representation of Individual Mobility Scenarios in Ad Hoc Networks and Its Evaluation, EURASIP Journal on Wireless Communications and Networking, Vol. 2007, No. 1, Dec. 2007, p. 35946.

[20] A.H. Azni, R. Ahmad, Z.A.M. Noh, A.S.H. Bansari, B. Hussain: Correlated Node Behaviour Model based on Semi Markov Process for MANETS, IJCSI International Journal of Computer Science Issues, Vol. 9, No. 1, Jan. 2012, pp. 50 – 59.

[21] Z. Li, H. Shen: Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, Vol. 11, No. 8, Aug. 2012, pp. 1287 – 1303.