Egyptian Informatics Journal (2014) 15, 149–157

Cairo University

Egyptian Informatics Journal

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

ORIGINAL ARTICLE

Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for mitigating Selfish Nodes in MANETs

J. Sengathir *, R. Manoharan

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

Received 30 January 2014; revised 19 August 2014; accepted 31 August 2014
Available online 26 September 2014

KEYWORDS

Selfish nodes;
Exponential distribution;
Laplace Stleltjes Transform;
Survivability Coefficient;
Probability of cooperation

Abstract In MANETs, the cooperation is considered as an important entity for enabling reliable data dissemination among the mobile nodes. But, the existence of selfish nodes weakens the degree of cooperation and in turn reduces the network performance. Hence, the computation of reputation level for each and every node in the network becomes essential in order to make optimal routing decisions. In this paper, we propose a Laplace Stleltjes Transform based Conditional Survivability Coefficient Model (LCSCM), which manipulates the survivability of the network through a parameter called Conditional Survivability Coefficient (CSC). This Conditional Survivability Coefficient aids in determining the reputation level of mobile nodes as well as quantifies the survivability of the entire network. The performance of this conditional probabilistic approach is analyzed using ns-2 based on the network related parameters such as packet delivery ratio, throughput, total overhead, and control overhead by varying the number of mobile nodes in the network. The results obtained through these extensive simulations make it obvious that, this approach outperforms PCMA model with a successful detection rate of 24%. This LCSCM also facilitates in framing 0.25 as the saddle point for selfish node detection.

1. Introduction

In multi-hop networks like ad hoc network efficient data dissemination among mobile nodes necessitates maximum degree of collaboration [1]. Since the mobile nodes in MANETs are dynamic in nature and could drastically change its behavior, the maintenance of cooperation between nodes is crucial [2]. The various mechanisms contributed for mitigating misbehaving nodes in the literature have been formulated based on the concept that these nodes exploit the network resources without considering their own profit [3]. But, the selfish nodes make the

* 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

1110-8665 © 2014 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
http://dx.doi.org/10.1016/j.eij.2014.08.003

best out of the network resources for its own gain [4]. This kind of exploitation on the network resources by these nodes may result in performance degradation of the entire network [5]. Hence, a need arises for formulating a mathematical model which periodically computes the reputation level for each and every node that contributes in identifying the cooperation level of these nodes in the network.

In this paper, we contribute a Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for identifying and isolating selfish nodes. This conditional probabilistic model estimates the level of reputation for each and every mobile node through Conditional Survivability Coefficient (CSC). This coefficient computed based on second hand information obtained from neighbor nodes. This mathematical model also measures the survivability of the individual nodes present in the network based on two independent exponentially distributed parameters viz., the parameter for computing the failure rate of cooperative nodes and the parameter for computing the failure rate of selfish nodes. AODV protocol is used for studying the proposed mathematical model.

The remaining part of the paper is organized as follows. Section 2 summarizes the related works for detecting selfish nodes based on reputation factor computed by means of probability. Section 3 depicts the Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for isolating selfish nodes. Section 4 presents the algorithms used in the deployment of the proposed mathematical model in an ad hoc environment. Section 5 details on the illustration of the proposed model. The evaluation parameters setup for study and the experimental analysis are enumerated in Sections 6 and 7 respectively. Section 7.3 depicts the major contributions of the proposed model and Section 8 concludes the paper.

2. Related work

From the past decade, a number of probability based mathematical models have been contributed for detecting and mitigating selfish nodes. Some of those approaches are enumerated below:

A competent approach based on Bayesian theorem contributed by Buchegger and Boudec [6] for measuring the degree of reputation possessed by each and every node existing in an ad hoc scenario. Beta distribution, an adaptive version of Bernoulli distribution is utilized for calculating reputation rating for the mobile nodes. The nodes in the network are categorized into cooperative or selfish nodes based on a factor called threshold tolerance computed using the reputation ratings. They also considered priori probability set as $(1,1)$ and uniform distribution with $(0,1)$ for modeling the events. The authors have also addressed the various feasible vulnerabilities that could arise during reliable data dissemination between mobile nodes. Another trust based evidence model proposed by Kargl et al. [7] introduces a routing protocol called SDSR which makes each routing decisions based on the negotiation performed between mobile nodes in the network. This approach also possesses the capability of over hearing. The authors also introduce a secured architecture called SAM for detecting selfish nodes.

Further, Zouridaki et al. [8] proposed a novel frame work for checking the reliability of the packets forwarded by mobile nodes in an ad hoc scenario. The reputation level is computed based on first and second hand information obtained from neighbor nodes. The authors have used a factor called opinion metric for detecting malicious nodes. They have also used confidence and trust limits for making statistical prediction about the reliable delivery of data packets. Rizvi and Elleithy [9] proposed a mathematical model based on time division technique to reduce the malicious behavior of nodes.

Furthermore, Marti et al. [10] contributed a reputation framework based on watchdog and path rater. The author used neutral routing and suspected routing as two rating levels for identifying misbehaving nodes. Their mechanism mainly isolates the malicious nodes which are not cooperating rather than punishing them. Chen and Varatharajan [11] have proposed a selfish node detection mechanism based on Dempster-Shafer theory. Authors computed the cooperation level of nodes based on posterior probability. They also combined multiple evidences through a numerical procedure based on posterior probability.

Yet another, a collaborative mechanism called CORE proposed by Michiardi and Molva [12] utilized watch dog mechanism as the deduction component. They also incorporated three reputation categories viz., subjective reputation, indirect reputation and functional reputation for identifying the selfish based on their deviation of behavior. In addition, Hernandez-Orallo et al. [13] introduced a reputation based trust framework based on watchdog mechanism. The authors computed the detection time and total overhead that could originate due to the presence of selfish nodes through transition probability matrix. They also used two states namely NOINFO and POSITIVE based on continuous time Markov model.

Finally, the packet conservation monitoring algorithm (PCMA) contributed by Fahad and Askwith [14] is considered as the bench mark system for the proposed LCSCM approach due to the following reasons.

(a) It is the first monitoring algorithm attributed for detecting a special case of selfish nodes that drops packets partially based on the level of reputation.
(b) This mechanism relies only on the neighbors which have direct interaction with the suspicious nodes.
(c) This mechanism completely avoids any trust information obtained from the suspicious nodes, since it considers the suspicious nodes as untrustworthy.
(d) This mechanism decides a node as selfish when the number of packets forwarded by a mobile node to its neighbor is equal to the number of packets received by that node from its neighbors

2.1. Extract of the literature

The probabilistic mechanisms for mitigating selfish nodes present in the literature have the following pitfalls. They are

(a) A Laplace Stleltjes Transform based Conditional Reliability Coefficient Model for isolating selfish nodes has not been explored to the best of our knowledge.
(b) A conditional probability approach which makes optimal routing decisions in the existence of selfish nodes considering the survivability of individual nodes as well as the entire network has not been explored.

Hence, we have been motivated for proposing a probabilistic mathematical model for isolating selfish nodes so that the performance of the network could be enhanced.

3. Laplace Stleltjes Transform Based Conditional Survivability Coefficient Model (LCSCM)

In this section, we propose a Laplace Stleltjes Transform based Conditional Survivability Coefficient Model. This mathematical model makes use of a parameter called Conditional Survivability Coefficient (CSC), manipulated for estimating the reputation level of nodes present in the network. This probabilistic mechanism also aids in determining the impact of selfish nodes towards the survivability of the network.

Let 'x' be the overall lifetime of the nodes present in an ad hoc environment containing both cooperative nodes (normal nodes) and non-cooperative nodes (selfish nodes).

Suppose if '$P_r(i)$' and '$P_f(i)$', $1 \leqslant i \leqslant k$, be the number of packets received by a node from its neighbors and number of packets forwarded to its neighbor in 'k' sessions respectively.

The probability of cooperation identified for a node within the network lifetime 'x' is given by (1)

$$P_c = \frac{k\sum_{i=1}^{k} P_r(i) * P_f(i) - \sum_{i=1}^{k} P_r(i) \sum_{i=1}^{k} P_f(i)}{\sqrt{k\left(\sum_{i=1}^{k}(P_r(i))\right)^2 - \left(\sum_{i=1}^{k}(P_r(i))\right)^2} * \sqrt{k\left(\sum_{i=1}^{k}(P_f(i))\right)^2 - \left(\sum_{i=1}^{k}(P_f(i))\right)^2}} \tag{1}$$

where 'P_c' is the probability of cooperation identified for each node.

Let us assume 'r' as the random variable used for categorizing the nodes in an ad hoc network as cooperative and selfish based on the value of 'P_c'. If the 'P_c' value of a node reaches below a threshold of 0.50 as specified in [15], the node is said to exhibit selfish behavior with probability '$1 - P_c$'. At the same time, the node is cooperative with probability 'P_c', given by (2) and (3).

$$P_r(0) = P_c \tag{2}$$

$$P_r(1) = 1 - P_c \tag{3}$$

where, the random variable 'r' is defined as

$r = 0$, if a node is cooperative.

$r = 1$, if a node is selfish.

Let us consider an ad hoc network with 'n' nodes, in which 'k' are co-operative and 'n–k' are selfish.

Then, the rate of survivability for the entire network is given by (4)

$$\lambda = \frac{k}{n}(P_c) \tag{4}$$

and the rate of failure for the network is given by (5)

$$\mu = \frac{n-k}{n}(1 - P_c) \tag{5}$$

Under the constraints,

(a) 'k out of n' nodes are cooperative with probability P_c and

(b) '(n–k) out of n' nodes are selfish with probability $1 - P_c$.

The survivability of the entire network depends upon the lifetime of the normal node and the lifetime of the selfish node. Since, these two parameters are independent of each other and exponentially distributed the reputation for each and every individual node in the network could be manipulated by Laplace Stleltjes Transform [16]. Hence, the lifetime of the network 'x' is conditionally dependent on exponentially distributed with parameter $\lambda + \mu$.

Now, we define the probability mass function of 'r' by considering that the probability of a normal node for survivability is $\frac{\lambda}{\lambda+\mu}$ and the probability of a selfish node for survivability is $\frac{\mu}{\lambda+\mu}$.

Hence, the survivability expectation of a node to behave in normal mode is given by (6)

$$P_r(0) = \frac{\lambda(P_c)}{\lambda + \mu} \tag{6}$$

Therefore, the survivability of cooperative nodes within the network lifetime 'x' computed through Laplace Stleltjes Transform is given by Eq. (7) using Eq. (6).

$$L_{x_1}(r = 0) = (\lambda + \mu)e^{-(\lambda+\mu)t} \tag{7}$$

The survivability expectation of a node to be in selfish behavior within the network lifetime is given by (8).

$$P_r(1) = \frac{\mu(1 - P_c)}{\lambda + \mu} \tag{8}$$

Likewise, the survivability of selfish nodes within the network lifetime 'x' computed through Laplace Stleltjes is given by Eq. (9) using Eq. (8).

$$L_{x_2}(r = 1) = (\lambda + \mu)\lambda e^{-\lambda t} e^{-(\lambda+\mu)t} \tag{9}$$

Since, the survivability of the entire network depends on the survivability of both the cooperative nodes and selfish nodes, the Conditional Survivability Coefficient (CSC) for the entire network at any time 't' is computed using total theorem of probability is given by (10)

$$f_x(t) = \lambda e^{-(\lambda+\mu)t}(1 - P_c + \lambda P_c e^{-\lambda t}) \tag{10}$$

The presence of selfish nodes in the ad hoc environment increases exponentially, the value of CSC '$f_x(t)$' gradually decreases. When the value of CSC approaches to zero, network has to be rehabilitated. This Laplace Stleltjes Transform based Conditional Survivability Coefficient Model also aids in framing an optimal range for detecting selfish nodes.

4. Algorithms for Laplace Stleltjes Transform based Conditional Survivability Coefficient Model

The formulated Laplace Stleltjes based conditional reliability coefficient model is implemented using four algorithms viz., Algorithm 1 (estimation of probability of cooperation P_c), Algorithm 2 (estimation of rate of survivability λ and rate of failure μ), Algorithm 3 (estimation of CSC based on Laplace Stleltjes Transform) and Algorithm 4 (isolation of selfish nodes based on CSC).

Algorithm 1 elaborates the steps involved in estimating probability of cooperation P_c. The selfish behavior of nodes present in the ad hoc environment are identified based on the probability of cooperation 'P_c'. When the value of P_c reaches below 0.50 as defined in [15], then the node is designated as selfish.

Algorithm 1. Estimation of probability of cooperation 'P_c'.

Notations:

n – Total number of mobile nodes in the network.
N_i – Represents the node whose P_c has to be computed, where $1 \leqslant i \leqslant n$.
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.

Algorithm (estimation of P_c)

1. Begin
2. For each mobile node $i = 1$ to n do
3. Neighbor nodes of each N_i compute cooperativity coefficient P_c using $P_c = \frac{k\sum_{i=1}^{k} P_r(i)*P_f(i) - \sum_{i=1}^{k} P_r(i)\sum_{i=1}^{k} P_f(i)}{\sqrt{k(\sum_{i=1}^{k}(P_r(i)))^2 - \left(\sum_{i=1}^{k}(P_r(i))\right)^2} * \sqrt{k\left(\sum_{i=1}^{k}(P_f(i))\right)^2 - \left(\sum_{i=1}^{k}(P_f(i))\right)^2}}$
4. If the cooperativity coefficient of a mobile node ($N_i(P_c) < 0.5$) then
5. N_i is a selfish node
6. Else
7. N_i is a cooperative node
8. End If
9. End for
10. End

Algorithm 2 enumerates on the estimation of rate of survivability (λ) and rate of failure (μ). This algorithm determines the total number of selfish nodes and total number of cooperative nodes present in the network as c and s respectively. The survivability of the entire network (λ) and the failure rate for the network (μ) is manipulated with the aid of 'P_c, c, s and n'. From the computed values of λ and μ, the survivability expectation of a node to be in cooperative behavior and survivability expectation of a node to be in selfish behavior are determined.

Algorithm 2. Estimation of rate of survivability λ and rate of failure μ.

Notations:

n – Total number of mobile nodes in the routing path.
N_i – Represents a node.
P_c – Probability of cooperation.
r – A random variable used to categorize selfish from cooperative.
c – Cooperative nodes.
s – Selfish nodes.

Algorithm (estimation of λ and μ)

1. Begin
2. For each and every mobile node $j = 1$ to n do
3. If $N_i(P_c) < 0.5$ then
4. Set the random variable (r) for nodes identified as selfish using $N_i(r) = 1$
5. Count the number of selfish nodes using $s = s + 1$
6. Else
7. Set the random variable (r) for that node as $N_i(r) = 0$
8. Count the number of cooperative nodes using $c = n - s$
9. End If
10. End for
11. Compute the rate of survivability for the entire network using $\lambda = \frac{c}{n}(P_c)$
12. Compute the rate of failure for the network using $\mu = \frac{n-c}{n}(1 - P_c)$
13. Compute the survivability expectation of a node to be in normal behavior using $P_r(0) = \frac{\lambda(P_c)}{\lambda+\mu}$
14. Compute the survivability expectation of a node to be in selfish behavior using $P_r(1) = \frac{\mu(1-P_c)}{\lambda+\mu}$
15. End

Algorithm 3 illustrates the steps in the estimation of CSC based on Laplace Stleltjes Transform using total theorem of probability. Initially, the survivability of cooperative nodes and selfish nodes are computed as S_c and S_s respectively. The Conditional Survivability Coefficient (CSC) for the entire network is manipulated with the aid of S_c, S_s, $P_r(0)$ and $P_r(1)$ values.

Algorithm 3. Estimation of CSC based on Laplace Stleltjes Transform.

Notations:

n – Total number of mobile nodes in the network.
t – Time instant.
r – A random variable representing the level of cooperation.
λ – The rate of survivability for the entire network.
μ – The rate of failure for the entire network.
S_c – Survivability of cooperative nodes.
S_s – Survivability of selfish nodes.
CSC – Conditional Survivability Coefficient.

Algorithm (computation of CSC)

1. Begin
2. for the entire network do
3. Compute survivability of cooperative nodes through Laplace Stleltjes Transform using $S_c = (\lambda + \mu)e^{-(\lambda+\mu)t}$
4. Compute the survivability of selfish nodes through Laplace Stleltjes Transforms using $S_s = (\lambda + \mu)\lambda e^{-\lambda t}e^{-(\lambda+\mu)t}$
5. Using S_c and S_s, compute the Conditional Survivability Coefficient based on total theorem of probability.
6. End for
7. End

The Algorithm 4 illustrates the steps involved in the decision of isolating selfish nodes based on CSC.

Algorithm 4. Isolation of selfish nodes based on CSC.

Notations

CSC – Conditional Survivability Coefficient.
R_{Th} – Threshold of rehabilitate.

Algorithm (isolate selfish node)

1. Begin
2. For every routing path in the network
3. If (CSC > R_{Th}), then
4. Isolate selfish nodes using Selfish _ rehabilitate ()
5. Else
6. Normal routing activity.
7. End for
8. End

When the CSC value for the entire network approaches to zero, the selfish nodes are mitigated using Selfish_rehabilitate (). As per the simulations conducted in this paper, the threshold of rehabilitate is determined as 0.01, since the network evaluation parameters degrades significantly at this point.

4.1. Correctness of the algorithm

The proposed Laplace Stleltjes Transform based Conditional Survivability Coefficient Model isolates selfish nodes through the computation of Conditional Survivability Coefficient (CSC) which is based on three factors viz., cooperativity coefficient (P_c), rate of survivability (λ) and rate of failure (μ). Moreover, these factors are directly computed through number of packets received by a node from its neighbors and number of packets forwarded by that node to its neighbor. Since this detection strategy purely depends only on the rate of packet delivery of a mobile node, it does not possess any false negative and false positive probabilities for detecting selfish nodes.

5. Illustration of the proposed model

Consider an ad hoc environment containing both selfish and cooperative nodes. The nodes are classified based on the probability of cooperation 'P_c'. If the value of 'P_c' is less than 0.50 the nodes are identified as selfish ($r = 1$) else the nodes are identified as cooperative ($r = 0$). In this context, the reputation of each and every node monitored by their neighbors is illustrated with the aid of two possible scenarios.

Scenario 1. When the number of selfish node in the ad hoc environment are minimum.

Consider the group of nodes in AODV of the network as shown in Fig. 1. This topology contains 7 cooperative nodes ($k = 7$) and three selfish nodes ($m = n - k = 3$). Here, the rate of survivability 'λ' and rate of failure 'μ' for the entire network with (4) and (5) are computed as 0.42 and 0.12 respectively. The value of CSC for the entire network is computed as 0.029 using (10) with the help of survivability of cooperative nodes and selfish nodes computed through (7) and (9) respectively.

Since the value of CSC in Scenario 1 is greater than the threshold of rehabilitate, it infers that the impact of selfishness in the network survivability is minimum.

Scenario 2. When the number of selfish node in the ad hoc environment are maximum.

Consider the group of nodes in AODV of the network as shown in Fig. 2. This topology contains 3 cooperative nodes ($k = 3$) and three selfish nodes ($m = n - k = 7$). Here, the rate of survivability 'λ' and rate of failure 'μ' for the entire network with (4) and (5) are computed as 0.18 and 0.28 respectively.

The value of CSC for the entire network is computed as 0.009 using (10) with the help of survivability of cooperative nodes and selfish nodes computed through (7) and (9) respectively. Since the value of CSC in Scenario 2 is less than the threshold of rehabilitate, it infers that the impact of selfishness in the network survivability is maximum.

6. Simulation setup

Extensive simulations of LCSCM are carried out through $ns - 2.26$. In this simulation environment 100 mobile nodes were deployed in a terrain size of 1000×1000. The refresh interval time and the channel capacity for each simulation run are set as 10 s and 2 Mbps respectively. The following Table 1 depicts the simulation parameters setup for our study.

6.1. Evaluation parameters

The existence of selfish nodes decreases the survivability of the network by decreasing the packet delivery ratio and throughput while increasing the control overhead and total overhead. Hence, the formulated LCSCM is analyzed based on the following performance metrics enumerated below.

6.1.1. Packet delivery ratio

It may be defined as the ratio of total number of packets received by a node to the total number of packets actually destined for it.

6.1.2. Throughput

The aggregate number of data packets that are delivered at the destination node with in a time 't'.

6.1.3. Total overhead

It is defined as the ratio of total number of control and data packets required for connection establishment to the number of data packets that arrives the destination.

6.1.4. Control overhead

It is defined as the maximum size of the packets that are used for establishing the connection between the source node and destination node.

7. Experimental results and analysis

The experimental results depicts that maximum number of selfish nodes are detected, when the threshold value set for

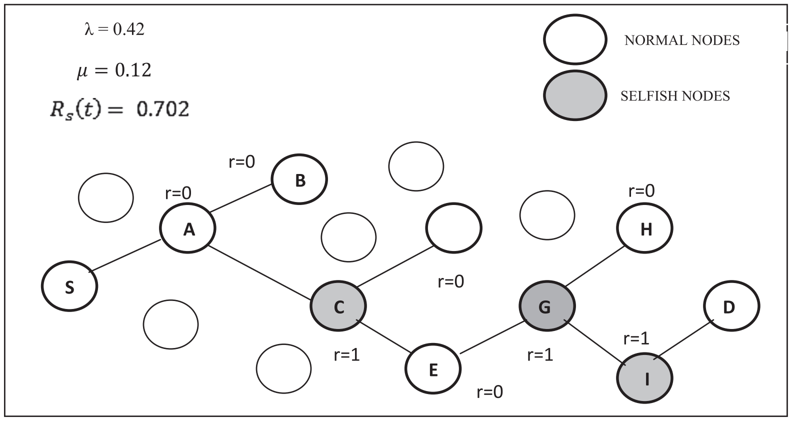

Figure 1 Group of nodes in AODV of the network (Scenario 1).

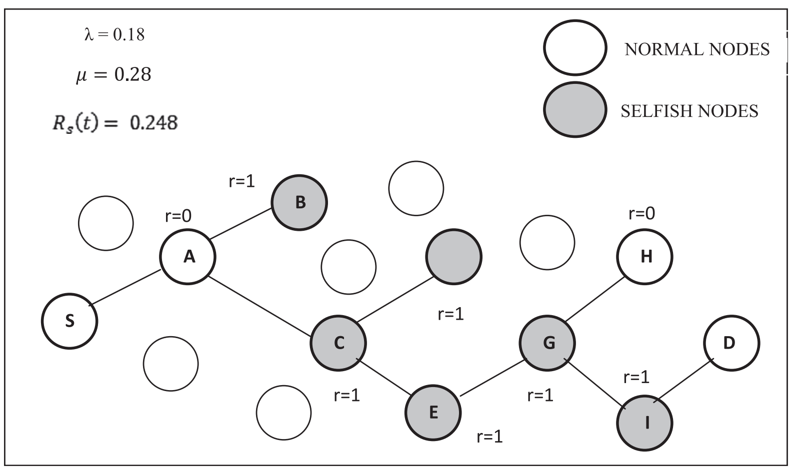

Figure 2 Group of nodes in AODV of the network (Scenario 2).

Table 1 Simulation Setup.

Parameter	Value	Description
No. of mobile nodes	100	Simulation node
Type of protocol	AODV	Channel type
Terrain area	$1000 \times 1000\ m^2$	Size of the terrain
Simulation time	100 s	Maximum simulation time
Traffic model	Constant bit rate	Type of traffic model used
Packet size	512 bytes	Size of the packets
Type of antenna	Antenna/Omni antenna	Antenna model
Type of propagation	Two ray ground	Radio propagation model

detection is 0.25. Fig. 3 interprets the possible number of selfish nodes that could be identified through LCSCM and PCMA by varying different values set for detection.

The maximum numbers of selfish nodes are detected, if the threshold value for detection is set in between 0.20 and 0.30. Hence, these values are considered as the maximum and minimum threshold value of the LCSCM proposed for detecting selfish nodes.

7.1. Performance analysis for LCSCM based on the varying the number of mobile nodes

7.1.1. Packet delivery ratio

The survivability of an ad hoc network highly depends upon the cooperation between nodes. When the number of selfish nodes increases exponentially packet delivery ratio decreases.

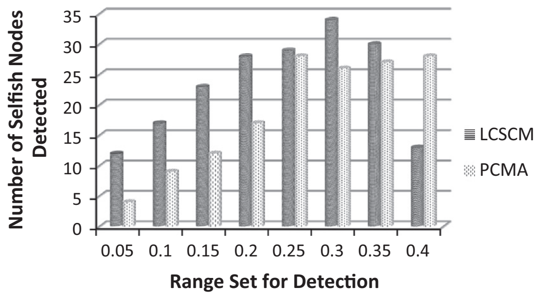

Figure 3 Chart representing the range set for identifying selfish nodes using LCSCM.

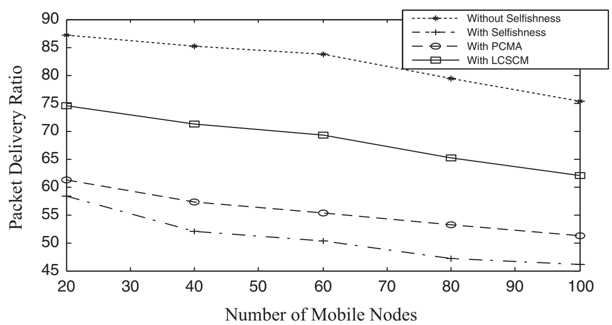

Figure 4 Performance analysis chart for LCSCM based on packet delivery ratio.

The deployment of this probabilistic model (LCSCM) in the network shows the phenomenal increase in packet delivery ratio when compared to the existing PCMA model. Fig. 4 depicts the performance of the network based on packet delivery ratio with the help of four schemes, viz., without selfishness, with selfishness, with PCMA and with LCSCM.

The proposed LCSCM scheme increases the packet delivery ratio to a maximum of 16% when compared to PCMA.

7.1.2. Throughput

The increase in number of selfish nodes in the network, decreases throughput of the entire network significantly. The deployment of this probabilistic model (LCSCM) in the network shows the phenomenal increase in throughput when compared to the existing PCMA model. Fig. 5 depicts the performance of the network based on throughput with the help of four schemes, viz., without selfishness, with selfishness, with PCMA and with LCSCM.

The proposed LCSCM scheme increases the throughput to a maximum of 14% when compared to PCMA.

7.1.3. Total overhead

The total overhead increases drastically, when the number of selfish nodes presents in an ad hoc scenario increases exponentially. The deployment of this probabilistic model (LCSCM) decreases the total overhead when compared to existing PCMA model. Fig. 6 depicts the performance of the network based on total overhead with the help of four schemes, viz., without selfishness, with selfishness, with PCMA and with LCSCM.

The proposed LCSCM scheme decreases the total overhead to a maximum of 17% when compared to PCMA.

7.1.4. Control overhead

The control overhead increases drastically, when the number of selfish nodes presents in an ad hoc scenario increases exponentially. The deployment of this probabilistic model (LCSCM) decreases the total overhead when compared to existing PCMA model. Fig. 7 depicts the performance of the network based on total overhead with the help of four schemes, viz., without selfishness, with selfishness, with PCMA and with LCSCM.

The proposed LCSCM scheme decreases the control overhead to a maximum of 27% when compared to PCMA.

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

7.2.1. Packet delivery ratio

The performance of the network decreases in terms of packet delivery ratio, when the number of selfish nodes present in an ad hoc scenario increases exponentially. Fig. 8 depicts the performance of the network based on packet delivery ratio with the help of three schemes, viz., with selfishness, with MIN threshold based detection for LCSCM and with MAX threshold based detection for LCSCM.

The deployment of LCSCM in the network increases the packet delivery ratio to an extent of 14% using minimum threshold based detection, while in case of maximum threshold based detection, it increases up to 29%.

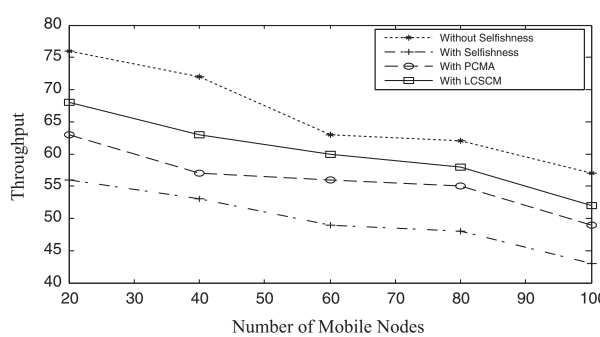

Figure 5 Performance analysis chart for LCSCM based on throughput.

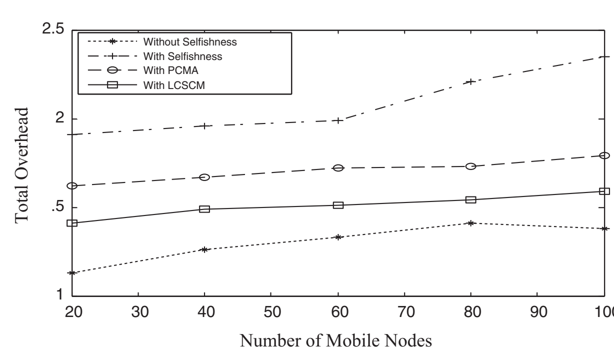

Figure 6 Performance analysis chart for LCSCM based on total overhead.

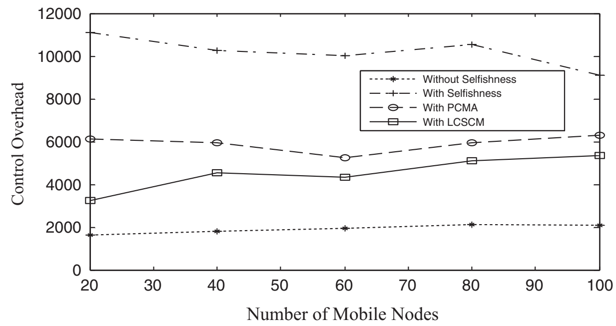

Figure 7 Performance analysis chart for LCSCM based on control overhead.

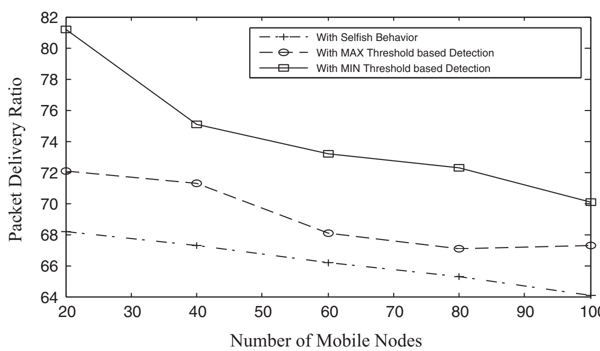

Figure 8 Performance analysis chart for LCSCM (MAX and MIN threshold) based on packet delivery ratio.

7.2.2. Throughput

The performance of the network decreases in terms of throughput, when the number of selfish nodes present in an ad hoc scenario increases exponentially. Fig. 9 depicts the performance of the network based on throughput with the help of three schemes, viz., with selfishness, with MIN threshold based detection for LCSCM and with MAX threshold based detection for LCSCM.

The deployment of LCSCM in the network increases the packet delivery ratio to an extent of 17% using minimum threshold based detection, while in case of maximum threshold based detection, it increases up to 25%.

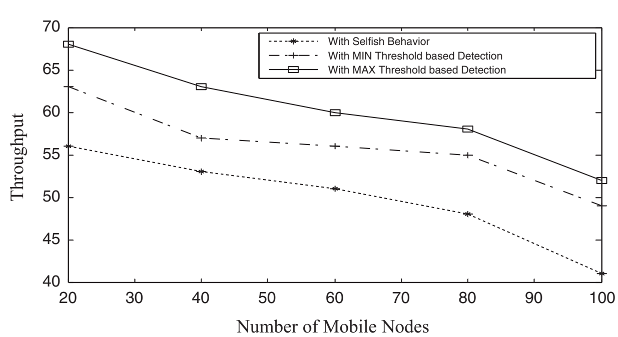

Figure 9 Performance analysis chart for LCSCM (MAX and MIN threshold) based on throughput.

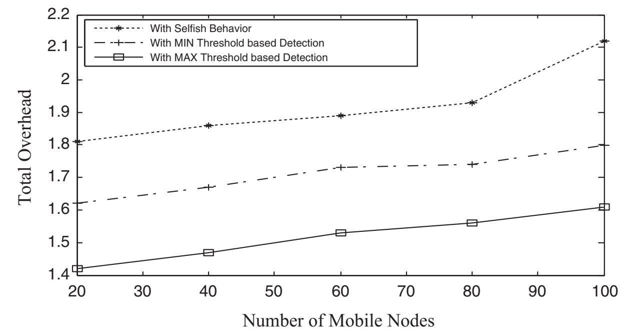

Figure 10 Performance analysis chart for LCSCM (MAX and MIN threshold) based on total overhead.

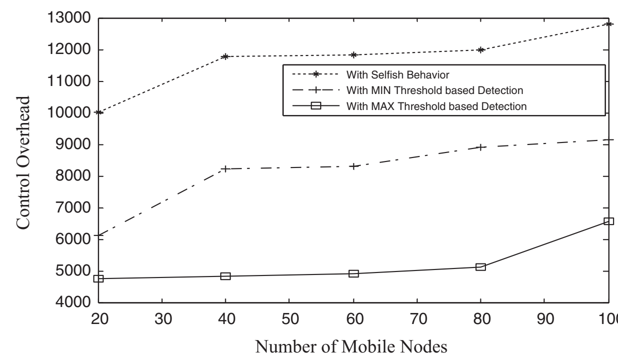

Figure 11 Performance analysis chart for LCSCM (MAX and MIN threshold) based on control overhead.

7.2.3. Total overhead

The total overhead increases drastically, when the number of selfish nodes presents in an ad hoc scenario increases exponentially. Fig. 10 depicts the performance of the network based on total overhead with the help of three schemes, viz., with selfishness, with MIN threshold based detection for LCSCM and with MAX threshold based detection for LCSCM.

The deployment of LCSCM in the network decreases the total overhead to an extent of 12% using minimum threshold based detection, while in case of maximum threshold based detection, it decreases up to 26%.

7.2.4. Control overhead

The control overhead increases drastically, when the number of selfish nodes presents in an ad hoc scenario increases exponentially. Fig. 11 depicts the performance of the network based on control overhead with the help of three schemes, viz., with selfishness, with MIN threshold based detection for LCSCM and with MAX threshold based detection for LCSCM.

The deployment of LCSCM in the network decreases the total overhead to an extent of 16% using minimum threshold based detection, while in case of maximum threshold based detection, it decreases up to 29%.

7.3. Major contributions of LCSCM

The major contributions of the proposed Laplace Stleltjes Transform based Conditional Survivability Coefficient Model are summarized as follows:

(a) We also infer that the probability of cooperation decreases when rate of survivability 'λ' decreases and rate of failure 'μ' increases.
(b) From the experimental analysis, we device a minimum and maximum value of detection as 0.30 and 0.20 respectively.
(c) We define a threshold value of detection for selfish nodes as 0.25, since the simulation results depicts that maximum number of selfish nodes are identified at this point of detection.

8. Conclusion

In this paper, the survivability of the network is studied with the help of Laplace Stleltjes Transform based Conditional Reliability Coefficient Model. The contributed LCSCM identifies the maximum number of selfish nodes when compared to the existing PCMA model available in the literature. In an average, the LCSCM approach has a successful detection rate of 24%, which is found to be remarkable. The experimental results makes it obvious that this conditional probabilistic approach outperforms the PCMA model in terms of packet delivery ratio, throughput, control overhead and total overhead.

References

[1] Buchegger S, Boudec J-Y. 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; 2002. p. 234–42.
[2] Campos CV, de Moraes M. A Morkovian model representation of individual mobility scenarios in ad hoc networks and its evaluation. EURASIP J Wireless Commun Netw 2012;1(3):231–5292.
[3] Li Ze, Shen Haiying. Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. IEEE Trans Mob Comput 2012;11(8):110–2.
[4] Azni AH, Ahmad Rabiah, Noh Zul Azri Muhamad, Basari Abd Samad Hasan, Hussin Burairah. Correlated node behavior model based on semi markov process for MANETS. IJCSI Int J Computr Sci Issues 2012;9(1):212–22.
[5] Buttyan L, Hubaux J-P. Stimulating cooperation in self-organizing mobile ad hoc networks. MONET J Mob Comput Netw 2003;8(1):579–92.
[6] 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.
[7] 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.
[8] Zouridaki C, Mark BL, Hejmo M, Thomas RK. 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; 2009. p. 1–10.
[9] Rizvi S, Elleithy M. A new scheme for minimizing malicious behavior of mobile nodes in mobile ad hoc networks. Int J Comput Sci Inf Security 2009;3(1):25–34.
[10] Marti S, Gulli TJ, Lai K, Baker M. 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; 2000. p. 255–65.
[11] Chen TM, Varatharajan V. Dempster–Shafer theory for intrusion detection in ad hoc networks. IEEE Internet Comput 2009;3(1):234–41.
[12] 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.
[13] Hernandez-Orallo, Serrat Manuel D, Cano Juan-Carlos, Calafate T, Manzoni. Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Commun Lett 2012;16(5):123–31.
[14] 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.
[15] Akhtar Md Amir Khusru, 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.
[16] Steutel FW, Van Harn K. Infinite divisibility of probability distributions on the real line. Marcer Dekker; 2004.