

[Egyptian Informatics Journal (2014) 15, 149](http://dx.doi.org/10.1016/j.eij.2014.08.003)–[157](http://dx.doi.org/10.1016/j.eij.2014.08.003)

Cairo University

Egyptian Informatics Journal

[www.elsevier.com/locate/eij](http://www.elsevier.com/locate/eij) [www.sciencedirect.com](http://www.sciencedirect.com/science/journal/11108665)

ORIGINAL ARTICLE

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



J. Sengathir [\*](#_bookmark0), 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

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 param- eter 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.

© 2014 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information,

KEYWORDS

Selfish nodes; Exponential distribution;

Laplace Stleltjes Transform; Survivability Coefficient; Probability of cooperation

Cairo University.

1. Introduction

\* Corresponding author. Tel.: +91 9940808674.

E-mail addresses: [j.sengathir@gmail.com](mailto:j.sengathir@gmail.com) (J. Sengathir), [rmanohar-](mailto:rmanoharan@pec.edu) [an@pec.edu](mailto:rmanoharan@pec.edu) (R. Manoharan).

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

**Production and hosting by Elsevier**

In multi-hop networks like ad hoc network efficient data dis- semination among mobile nodes necessitates maximum degree of collaboration [[1]](#_bookmark28). 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]](#_bookmark34). The various mechanisms contributed for mitigating misbehav- ing nodes in the literature have been formulated based on the concept that these nodes exploit the network resources without considering their own profit [[3]](#_bookmark35). But, the selfish nodes make the

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]](#_bookmark36). This kind of exploitation on the network resources by these nodes may result in performance degradation of the entire network [[5]](#_bookmark29). 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 identi- fying 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 infor- mation obtained from neighbor nodes. This mathematical model also measures the survivability of the individual nodes present in the network based on two independent exponen- tially 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 isolat- ing 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 Sec- tions 6 and 7 respectively. Section 7.3 depicts the major con- tributions of the proposed model and Section 8 concludes the paper.

1. Related work

From the past decade, a number of probability based mathe- matical models have been contributed for detecting and miti- gating selfish nodes. Some of those approaches are enumerated below:

A competent approach based on Bayesian theorem contrib- uted by Buchegger and Boudec [[6]](#_bookmark29) for measuring the degree of reputation possessed by each and every node existing in an ad hoc scenario. Beta distribution, an adaptive version of Ber- noulli 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 uni- form 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]](#_bookmark29) 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]](#_bookmark29) 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 con- fidence and trust limits for making statistical prediction about the reliable delivery of data packets. Rizvi and Elleithy [[9]](#_bookmark29) proposed a mathematical model based on time division tech- nique to reduce the malicious behavior of nodes.

Furthermore, Marti et al. [[10]](#_bookmark29) 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]](#_bookmark30) have pro- posed a selfish node detection mechanism based on Demp- ster-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 pro- posed by Michiardi and Molva [[12]](#_bookmark31) utilized watch dog mecha- nism 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]](#_bookmark32) introduced a reputation based trust frame- work 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 proba- bility 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]](#_bookmark33) is considered as the bench mark system for the proposed LCSCM approach due to the following reasons.

1. It is the first monitoring algorithm attributed for detect- ing a special case of selfish nodes that drops packets par- tially based on the level of reputation.
2. This mechanism relies only on the neighbors which have direct interaction with the suspicious nodes.
3. This mechanism completely avoids any trust informa- tion obtained from the suspicious nodes, since it consid- ers the suspicious nodes as untrustworthy.
4. This mechanism decides a node as selfish when the num- ber of packets forwarded by a mobile node to its neigh- bor is equal to the number of packets received by that node from its neighbors
   1. *Extract of the literature*

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

1. A Laplace Stleltjes Transform based Conditional Reli- ability Coefficient Model for isolating selfish nodes has not been explored to the best of our knowledge.
2. A conditional probability approach which makes opti- mal 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 probabilis- tic mathematical model for isolating selfish nodes so that the performance of the network could be enhanced.

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

In this section, we propose a Laplace Stleltjes Transform based Conditional Survivability Coefficient Model. This mathemati- cal model makes use of a parameter called Conditional Surviv- ability Coefficient (CSC), manipulated for estimating the reputation level of nodes present in the network. This probabi- listic 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 ‘*Pr*(*i*)’ and ‘*Pf*(*i*)’, 1 6 *i* 6 *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)](#_bookmark1)

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]](#_bookmark38). Hence, the lifetime of the net- work ‘*x*’ is conditionally dependent on exponentially distrib- uted with parameter k + l.

Now, we define the probability mass function of ‘*r*’ by con- sidering that the probability of a normal node for survivability is k and the probability of a selfish node for survivability is

k

l +l

k+l.

Hence, the survivability expectation of a node to behave in normal mode is given by [(6)](#_bookmark2)

k(*Pc*)

*Pr*(0) = k + l (6)

Therefore, the survivability of cooperative nodes within the network lifetime ‘*x*’ computed through Laplace Stleltjes Trans- form is given by Eq. [(7)](#_bookmark3) using Eq. [(6)](#_bookmark2).

*Lx* (*r* = 0) = (k + l)*e*—(k+l)*t* (7)

1

*k*P*k P* (*i*)\* *P* (*i*)— P*k P* (*i*)P*k P* (*i*)

*P*

= *i*=1 *r f i*=1 *r i*=1 *f*

(1)

*c* rﬃﬃﬃ ﬃﬃﬃPﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃ2ﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃPﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃ2**ﬃ** rﬃﬃﬃ ﬃﬃﬃPﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃ2ﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃPﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃ2**ﬃ**

*k*

*k i*=1

(*Pr*(*i*))

—

*k i*=1

(*Pr*(*i*))

\*

*k*

*k i*=1

(*Pf*(*i*))

—

*k i*=1

(*Pf*(*i*))

where ‘*Pc*’ is the probability of cooperation identified for each node.

Let us assume ‘*r*’ as the random variable used for categoriz-

The survivability expectation of a node to be in selfish behavior within the network lifetime is given by [(8)](#_bookmark4).

l(1 — *Pc*)

ing the nodes in an ad hoc network as cooperative and selfish

based on the value of ‘*Pc*’. If the ‘*Pc*’ value of a node reaches

*Pr*(1) =

(8)

k + l

below a threshold of 0.50 as specified in [[15]](#_bookmark37), the node is said to exhibit selfish behavior with probability ‘1 — *Pc*’. At the same time, the node is cooperative with probability ‘*Pc*’, given by [(2) and (3)](#_bookmark6).

*Pr*(0) = *Pc* (2)

*Pr*(1) = 1 — *Pc* (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)](#_bookmark8)

*k*

k = *n* (*Pc*) (4)

and the rate of failure for the network is given by [(5)](#_bookmark9)

l = *n* — *k* (1 — *P* ) (5)

Likewise, the survivability of selfish nodes within the net-

work lifetime ‘*x*’ computed through Laplace Stleltjes is given by Eq. [(9)](#_bookmark5) using Eq. [(8)](#_bookmark4).

*Lx* (*r* = 1) = (k + l)k*e*—k*te*—(k+l)*t* (9)

2

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)](#_bookmark7)

*fx*(*t*) = k*e*—(k+l)*t*(1 — *Pc* + k*Pce*—k*t*) (10)

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

1. Algorithms for Laplace Stleltjes Transform based Conditional

*n c* Survivability Coefficient Model

Under the constraints,

1. ‘*k* out of *n*’ nodes are cooperative with probability *Pc*

and

1. ‘(*n*–*k*) out of *n*’ nodes are selfish with probability 1 — *Pc*.

The formulated Laplace Stleltjes based conditional reliability coefficient model is implemented using four algorithms viz., [Algorithm 1](#_bookmark10) (estimation of probability of cooperation *Pc*),

[Algorithm 2](#_bookmark12) (estimation of rate of survivability k and rate of failure l), [Algorithm 3](#_bookmark11) (estimation of CSC based on Laplace Stleltjes Transform) and [Algorithm 4](#_bookmark13) (isolation of selfish nodes based on CSC).

[Algorithm 1](#_bookmark10) elaborates the steps involved in estimating probability of cooperation *Pc*. The selfish behavior of nodes present in the ad hoc environment are identified based on

the probability of cooperation ‘*P* ’. When the value of *P*

1. Begin
2. For each and every mobile node *j* =1 to *n* do
3. If *Ni*(*Pc*) < 0.5 then
4. Set the random variable (*r*) for nodes identified as selfish using

*Ni*(*r*)= 1

1. Count the number of selfish nodes using *s* = *s* +1
2. Else
3. Set the random variable (*r*) for that node as *Ni*(*r*)= 0
4. Count the number of cooperative nodes using *c* = *n* — *s*
5. End If
6. End for
7. Compute the rate of survivability for the entire network using

k = *c* (*Pc*)

*n*

12. Compute the rate of failure for the network using

*n*

13. Compute the survivability expectation of a node to be in normal

l = *n*—*c* (1 — *Pc*)

behavior using *Pr*(0) = k(*Pc* )

k+l

14. Compute the survivability expectation of a node to be in selfish

behavior using *Pr*(1) = l(1—*Pc* )

k+l

15. End

*c* – Cooperative nodes.

*s* – Selfish nodes.

Algorithm (estimation of k and l)

*c c*

reaches below 0.50 as defined in [[15]](#_bookmark37), then the node is desig-

nated as selfish.

Algorithm 1. Estimation of probability of cooperation ‘*Pc*’.

Notations:

*n* – Total number of mobile nodes in the network.

*Ni* – Represents the node whose *Pc* has to be computed, where 1 6 *i* 6 *n*.

*Pf* – Number of packets forwarded by a mobile node to its neighbors.

*Pr* – Number of packets received by a mobile node from its

neighbors.

*k* – Number of sessions.

Algorithm (estimation of *Pc*)

1. Begin
2. For each mobile node *i* =1 to *n* do
3. Neighbor nodes of each *Ni* compute cooperativity coeﬃcient *Pc*

using *P* =

*i*=1

*c*

P

*k*

2

P*k*

ÿ

P

*k*

ÿ

2

P P

*k k*

qﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃqﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ

*k P* (*i*)\**P* (*i*)— *P* (*i*) *P* (*i*)

*r f r f*

*i*=1 *i*=1

\* *k*

P

ÿ

2

P

*k*

2

*k*(

*i*=1

(*Pr* (*i*))) — (*Pr* (*i*)) *k*

*i*=1

*i*=1

(*Pf* (*i*)) — (*Pf* (*i*))

*i*=1

1. If the cooperativity coeﬃcient of a mobile node (*Ni*(*Pc*) < 0.5)

then

1. *Ni* is a selfish node
2. Else
3. *Ni* is a cooperative node
4. End If
5. End for
6. End

ﬃ

[Algorithm 2](#_bookmark12) enumerates on the estimation of rate of surviv- ability (k) and rate of failure (l). 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 sur- vivability of the entire network (k) and the failure rate for the network (l) is manipulated with the aid of ‘*Pc*, *c*, *s* and *n*’. From the computed values of k and l, the survivability expectation of a node to be in cooperative behavior and surviv- ability expectation of a node to be in selfish behavior are determined.

Algorithm 2. Estimation of rate of survivability k and rate of failure l.

Notations:

*n* – Total number of mobile nodes in the routing path.

*Ni* – Represents a node.

*Pc* – Probability of cooperation.

*r* – A random variable used to categorize selfish from cooperative.

[Algorithm 3](#_bookmark11) 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 *Sc* and *Ss* respectively. The Conditional Survivability Coefficient (CSC) for the entire network is manipulated with the aid of *Sc*, *Ss*, *Pr*(0) and *Pr*(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.

k – The rate of survivability for the entire network.

l – The rate of failure for the entire network.

*Sc* – Survivability of cooperative nodes.

*Ss* – 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 *Sc* = (k + l)*e*—(k+l)*t*
4. Compute the survivability of selfish nodes through Laplace Stleltjes Transforms using *Ss* = (k + l)k*e*—k*te*—(k+l)*t*
5. Using *Sc* and *Ss*, compute the Conditional Survivability Coeﬃcient based on total theorem of probability.
6. End for
7. End

The [Algorithm 4](#_bookmark13) illustrates the steps involved in the deci- sion of isolating selfish nodes based on CSC.

Algorithm 4. Isolation of selfish nodes based on CSC. Notations

CSC – Conditional Survivability Coefficient.

*RTh* – Threshold of rehabilitate.

Algorithm (isolate selfish node)

1. Begin
2. For every routing path in the network
3. If (CSC > *RTh*), 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 thresh- old of rehabilitate is determined as 0.01, since the network evaluation parameters degrades significantly at this point.

* 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 coef- ficient (*Pc*), rate of survivability (k) and rate of failure (l). Moreover, these factors are directly computed through num- ber of packets received by a node from its neighbors and num- ber 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.

1. Illustration of the proposed model

Consider an ad hoc environment containing both selfish and cooperative nodes. The nodes are classified based on the prob- ability of cooperation ‘*Pc*’. If the value of ‘*Pc*’ 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 reputa- tion 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](#_bookmark16). This topology contains 7 cooperative nodes (*k* = 7) and three selfish nodes (*m* = *n* — *k* = 3). Here, the rate of survivability ‘k’ and rate of failure ‘l’ for the entire net- work with [(4) and (5)](#_bookmark8) are computed as 0.42 and 0.12 respec- tively. The value of CSC for the entire network is computed as 0.029 using [(10)](#_bookmark7) with the help of survivability of cooperative nodes and selfish nodes computed through [(7) and (9)](#_bookmark3) respectively.

Since the value of CSC in [Scenario 1](#_bookmark15) 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](#_bookmark17). This topology contains 3 cooperative nodes (*k* = 3) and three selfish nodes (*m* = *n* — *k* = 7). Here, the rate of survivability ‘k’ and rate of failure ‘l’ for the entire net- work with [(4) and (5)](#_bookmark8) are computed as 0.18 and 0.28 respectively.

The value of CSC for the entire network is computed as

0.009 using [(10)](#_bookmark7) with the help of survivability of cooperative nodes and selfish nodes computed through [(7) and (9)](#_bookmark3) respec- tively. Since the value of CSC in [Scenario 2](#_bookmark14) is less than the threshold of rehabilitate, it infers that the impact of selfishness in the network survivability is maximum.

1. 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](#_bookmark18) depicts the simulation parameters setup for our study.

* 1. *Evaluation parameters*

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

* + 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 des- tined for it.

* + 1. *Throughput*

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

* + 1. *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.

* + 1. *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.

1. Experimental results and analysis

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

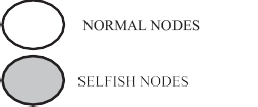
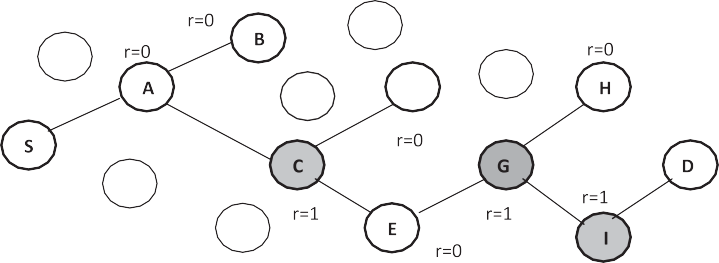


Figure 1 Group of nodes in AODV of the network ([Scenario 1](#_bookmark15)).

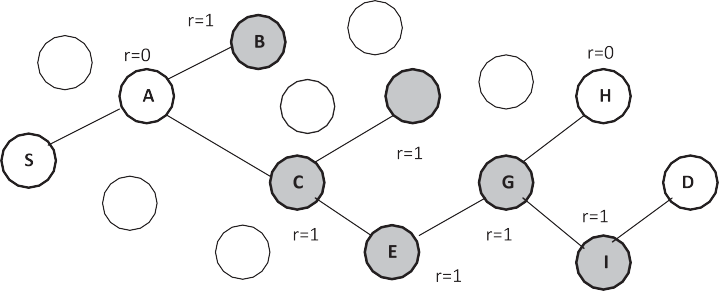


Figure 2 Group of nodes in AODV of the network ([Scenario 2](#_bookmark14)).

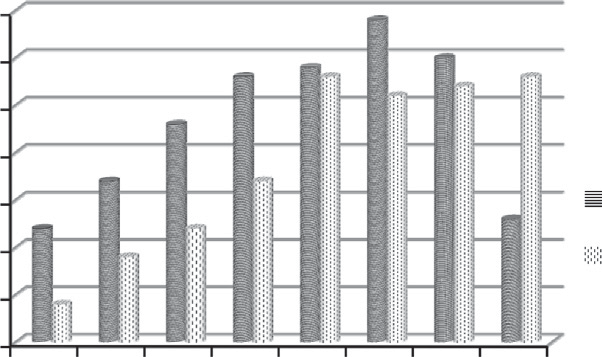
|  |  |  |
| --- | --- | --- |
| Table 1 Simulation Setup. |  | |
| Parameter | Value | Description |
| No. of mobile nodes | 100 | Simulation node |
| Type of protocol | AODV | Channel type |
| Terrain area | 1000 · 1000 m2 | Size of the terrain |
| Simulation time | 100 s | Maximum simulation time |
| 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](#_bookmark19) interprets the possible number of self- ish 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 min- imum threshold value of the LCSCM proposed for detecting selfish nodes.

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

35

**Number of Selfish Nodes Detected**

30

25

20

15

10

5

0

0.05 0.1 0.15 0.2 0.25 0.3 0.35 0.4

**Range Set for Detection**

LCSCM PCMA

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 exponen- tially. The deployment of this probabilistic model (LCSCM) decreases the total overhead when compared to existing

Figure 3 Chart representing the range set for identifying selfish

nodes using LCSCM.

90

Without Selfishness With Selfishness With PCMA

With LCSCM

85

80

Packet Delivery Ratio

75

70

65

60

55

50

45

20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

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](#_bookmark20) depicts the performance of the network based on packet deliv- ery ratio with the help of four schemes, viz., without selfish- ness, 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.

* + 1. *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 net- work shows the phenomenal increase in throughput when compared to the existing PCMA model. [Fig. 5](#_bookmark21) depicts the

PCMA model. [Fig. 6](#_bookmark22) 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 expo- nentially. The deployment of this probabilistic model (LCSCM) decreases the total overhead when compared to existing PCMA model. [Fig. 7](#_bookmark23) 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 over- head to a maximum of 27% when compared to PCMA.

* 1. *Performance analysis for LCSCM based on maximum and minimum threshold by varying the number of mobile nodes*
     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](#_bookmark25) 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%.

80

Without Selfishness With Selfishness With PCMA

With LCSCM

75

70

65

Throughput

60

55

50

45

40

20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

2.5

2

Total Overhead

.5

1

Without Selfishness With Selfishness With PCMA

With LCSCM

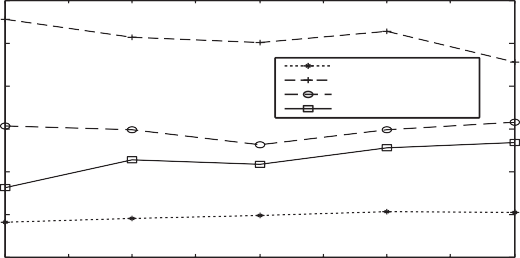
20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

Figure 5 Performance analysis chart for LCSCM based on throughput.

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

12000



Without Selfishness With Selfishness With PCMA

With LCSCM

10000

8000

Control Overhead

6000

4000

2000

0

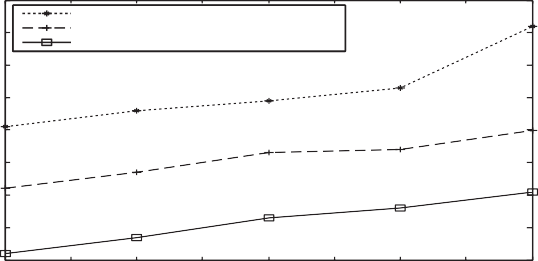
20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

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

2.2

2.1



With Selfish Behavior

With MIN Threshold based Detection With MAX Threshold based Detection

2

Total Overhead

1.9

1.8

1.7

1.6

1.5

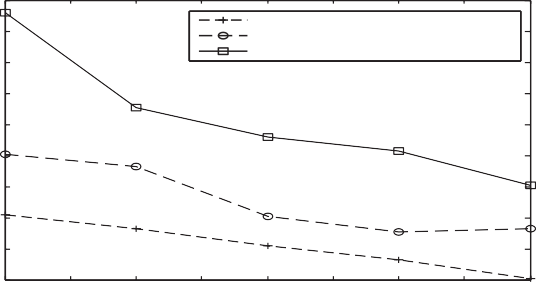
1.4

20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

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

82



With Selfish Behavior

With MAX Threshold based Detection With MIN Threshold based Detection

80

78

Packet Delivery Ratio

76

74

72

70

68

66

64

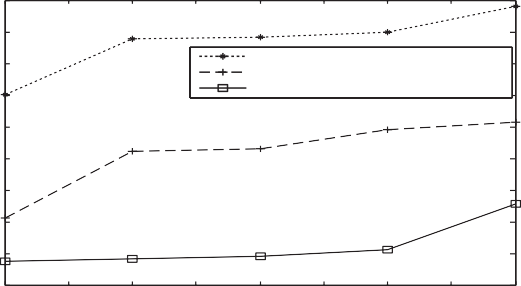
20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

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

13000

12000



With Selfish Behavior

With MIN Threshold based Detection With MAX Threshold based Detection

11000

Control Overhead

10000

9000

8000

7000

6000

5000

4000

20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

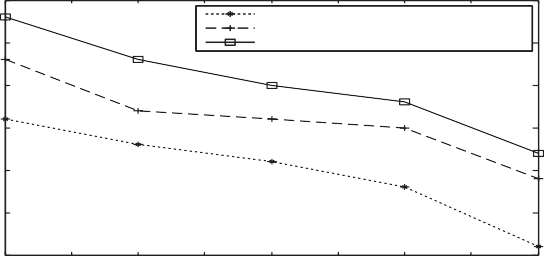
Figure 11 Performance analysis chart for LCSCM (MAX and MIN threshold) based on control overhead.

* + 1. *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](#_bookmark27) depicts the per- formance 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 detec- tion 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%.

70



With Selfish Behavior

With MIN Threshold based Detection With MAX Threshold based Detection

65

60

Throughput

55

50

45

40

20 30 40 50 60 70 80 90 100

Number of Mobile Nodes

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

* + 1. *Total overhead*

The total overhead increases drastically, when the number of selfish nodes presents in an ad hoc scenario increases exponen- tially. [Fig. 10](#_bookmark24) depicts the performance of the network based on total overhead with the help of three schemes, viz., with selfish- ness, 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%.

* + 1. *Control overhead*

The control overhead increases drastically, when the number of selfish nodes presents in an ad hoc scenario increases expo- nentially. [Fig. 11](#_bookmark26) 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%.

* 1. *Major contributions of LCSCM*

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

1. We also infer that the probability of cooperation decreases when rate of survivability ‘k’ decreases and rate of failure ‘l’ increases.
2. From the experimental analysis, we device a minimum and maximum value of detection as 0.30 and 0.20 respectively.
3. We define a threshold value of detection for selfish nodes as 0.25, since the simulation results depicts that maxi- mum number of selfish nodes are identified at this point of detection.
4. 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 identi- fies 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](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0010) [individual mobility scenarios in ad hoc networks and its evalu-](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0010) [ation. EURASIP J Wireless Commun Netw 2012;1(3):231–5292](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0010).
3. [Li Ze, Shen Haiying. Game-theoretic analysis of cooperation](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0015) [incentive strategies in mobile ad hoc networks. IEEE Trans Mob](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0015) [Comput 2012;11(8):110–2](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0015).
4. [Azni AH, Ahmad Rabiah, Noh Zul Azri Muhamad, Basari Abd](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0020) [Samad Hasan, Hussin Burairah. Correlated node behavior model](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0020) [based on semi markov process for MANETS. IJCSI Int J](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0020) [Computr Sci Issues 2012;9(1):212–22](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0020).
5. [Buttyan L, Hubaux J-P. Stimulating cooperation in self-organiz-](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0025) [ing mobile ad hoc networks. MONET J Mob Comput Netw](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0025) [2003;8(1):579–92](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0025).
6. Buchegger S, Boudec J-Y. Performance analysis of the CONFI- DANT 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](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0045) [behavior of mobile nodes in mobile ad hoc networks. Int J](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0045) [Comput Sci Inf Security 2009;3(1):25–34](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0045).
10. Marti S, Gulli TJ, Lai K, Baker M. Mitigating routing misbe- havior 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](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0055) [detection in ad hoc networks. IEEE Internet Comput](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0055) [2009;3(1):234–41](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0055).
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.

1. [Hernandez-Orallo, Serrat Manuel D, Cano Juan-Carlos, Calafate](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0065) [T, Manzoni. Improving selfish node detection in MANETs using](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0065) [a collaborative watchdog. IEEE Commun Lett 2012;16(5):123–31](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0065).
2. 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 telecommunica- tions, networking and broadcasting (PGNet), vol. 1, no. 1; 2006.

p. 78–84.

1. [Akhtar Md Amir Khusru, Sahoo G. Classification of selfish and](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0075) [regular nodes based on reputation values in MANET using](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0075) [adaptive decision boundary. Sci Res J Commun Netw](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0075) [2013;5(1):185–91](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0075).
2. [Steutel FW, Van Harn K. Infinite divisibility of probability](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0080) [distributions on the real line. Marcer Dekker; 2004](http://refhub.elsevier.com/S1110-8665(14)00031-0/h0080).