Journal of Engg. Research **Vol. 4 No. (1) March 2016** pp. 43-64

عامل الأُس التأكيدي المبني على ميكانيكية التخفيف للعقد الذاتية في شبكات الموبايل الخاصة (MANET)

ج. سينجاثر ور. مانوهاران
قسم علوم وهندسة الكمبيوتر، كلية بونديشري للهندسة، الهند

الخلاصة

إن النقل المعتبر للمعلومات في شبكات الموبايل الخاصة يعتمد أساساً على التعاون بين جميع عقد الموبايل النشطة في الشبكة. ولكن إرغام عقدة ما للمساهمة مع باقي عقد الموبايل مهمة صعبة. وإضافة إلى ذلك، عقد الموبايل في أي شبكة خاصة لديها طاقة بطارية محدودة لذلك ترفض العقد نقل حزم العقد المجاورة من أجل المحافظة على طاقتها. هذا التصرف "الأناني" لعقد الموبايل تقلل درجة المشاركة بين عقد الموبايل النشطة مما يؤثر على أداء الشبكة. لذلك تبرز الحاجة لتكوين ميكانيكية سمعية تساعد على عزل العقد "الأنانية" في شبكات الموبايل الخاصة. في هذة الورقة.. يقترح الباحثان معامل أُسي معتمد مبني على ميكانيكية التخفيف للتعرف وعزل العقد "الأنانية". هذا المعامل يعزل هذة العقد بفعالية بمساعدة المعامل الأُسي المعتمد الذي يحسب بناء على المعلومات الأولى والثانية التي يتم الحصول عليها من عقد الموبايل.الأداء الفعال لهذا المعامل تم دراستة بشمولية من خلال نموذجين حسابيين والنتائج التي تم الحصول عليها بينت أن المعامل قام بعزل العقد "الأنانية" بسرعة أكبر بمقدار (36%) من ميكانيكية التخفيف الأخري من الطريقة المبنية على التسجيل والثقة وطريقة ميكانيكية المعامل الموثق وطريقة خوارزمية متابعة الحزم المحافظة. الدراسة الأنموذجية هذه أظهرت أداء أفضل للشبكة بنسب 21%، 29%، 34% مقارنة بإستخدام الطرق الثلاث المذكورة أعلاه.

Exponential reliability factor based mitigation mechanism for selfish nodes in MANETs

J. Sengathir* and R. Manoharan

Department of Computer Science and Engineering, Pondicherry Engineering College,

East Coast Road, Pillaichavady, Puducherry, INDIA

**Corresponding author: j.sengathir@gmail.com*

ABSTRACT

Reliable dissemination of data in mobile ad hoc networks mainly depends on the cooperation among all the active mobile nodes present in the network. However, enforcing a node to cooperate with all the other mobile nodes is a difficult task. Moreover, the mobile nodes in an ad hoc network have limited battery power and hence they refuse to forward their neighbor nodes' packets so as to conserve their energy. This intentional selfish behavior of mobile nodes reduces the degree of cooperation between active mobile nodes which in turn affects the network performance. Hence, a need arises for formulating a reputation mechanism which helps in isolating selfish nodes in MANETs. In this paper, we propose an Exponential Reliability Factor Based Mitigation Mechanism (ERFBM) for detecting and isolating selfish nodes. This ERFBM efficiently isolates selfish nodes with the aid of Exponential Reliability Factor (ERF) computed based on the first and second hand information obtained from the mobile nodes. The effective performance of ERFBM is extensively studied through ns-2 simulations and the results obtained clearly portray that the proposed ERFBM isolates selfish nodes at a faster rate of 36% than the considered benchmark mitigation mechanisms such as Record and Trust-Based Detection (RTBD), Reliability Factor Based Mitigation Mechanism (RFBMM) and Packet Monitoring Conservation Algorithm (PCMA). The simulation study also depicts that ERFBM on an average, improves the performance of the network by reducing the communication overhead by 21%, 29% and 34% more than the three benchmark mitigation mechanisms considered for investigation.

Keywords: Available energy metric; exponential reliability factor; Mobile Ad Hoc Network (MANET); moving average method; selfish nodes.

INTRODUCTION

In MANETs, the mobile nodes collaborate with each other in order to forward the packet from the source node to the destination node (*Azni et al., 2012*). Since the

topology of ad hoc network is dynamic in nature, providing security to this type of network has received high degree of interest in the recent past. Most of the proposed approaches for isolating selfish nodes in the literature assume that malicious nodes exploit the network resources, without considering their own gain *(Campos & de Moraes, 2011*). In contrast, there is a class of mobile nodes called selfish nodes which exploit the network resources for its own benefits (*Li & Shen, 2012*). Further, the selfish nodes are classified into TYPE I, TYPE II and TYPE III selfish nodes *(Kumar & Bahadhur, 2013)*. TYPE I selfish nodes actively cooperate in the route establishment process but do not forward data packets to their neighbour nodes, while TYPE II selfish nodes cooperate neither in route establishment nor in data transmission. TYPE III selfish nodes on the other hand, drop data packets due to its limited availability of residual energy (*Roy & Chaki, 2011a*).

Furthermore, TYPE I and TYPE III selfish nodes are considered to be more vulnerable since they directly affect the performance of the network by drastically reducing the degree of cooperation established between the mobile nodes (*Amir Khusru et al., 2009*) in data dissemination. While, TYPE II selfish nodes are considered to be less vulnerable and mostly neglected by majority of the routing protocols proposed for ad hoc environment. In addition to this, a number of reputation based isolation schemes have been proposed in the literature for enhancing the degree of cooperation among the mobile nodes in the network under the influence of selfish behaviour of nodes (*Pusphalatha et al., 2009*). In general, these reputation schemes are classified into two broad categories viz., first hand and second hand reputation mechanisms. The first hand reputation approach monitors the node behaviour through direct interaction, while the second hand reputation approach identifies the node behaviour based on information obtained from the neighbours of the monitored node. Moreover, hybrid reputation mechansim is identified as an efficient and effective reputation mechanism, since it provides reliable information about a mobile node based on cumulative events as monitored by their direct and indirect (through neighbours) interaction.

Most of the mitigation mechanisms proposed for selfish nodes focus on either TYPE I or TYPE III selfish nodes. Further, an exponential distribution based second hand reputation mechanism that isolates TYPE I and TYPE III selfish nodes is not explored to the best of our knowledge. Hence, a need arises for formulating an energy based detection and isolation mechanism for Type I and Type III selfish nodes. This paper proposes an Exponential Reliability Factor Based Mitigation Mechanism (ERFBM) that could detect TYPE I and TYPE III selfish nodes in an ad hoc environment through second hand information. ERFBM incorporates a reactive protocol called AODV since it is predominantly uses adaptive routing protocol uniquely designed for an ad hoc network which performs sub-optimally to achieve reliability and improved performance.

Rest of the paper is organized as follows. Section 2 details on some of reputation based approaches proposed for mitigating selfish nodes present in the literature. Section 3 presents the Exponential Reliability Factor Based Mitigation Mechanism and its associative algorithms that represent energy based selfish node detection, selfish node categorization and exponential reliability factor based selfish node isolation. Section 4 depicts the simulation and experimental analysis for the proposed Exponential Reliability Factor Based Selfish Node Mitigation Mechanism and section 5 concludes the paper with future plan of our work.

RELATED WORK

In the recent past, several reputation mechanisms for mitigating selfish nodes in an ad hoc network have been proposed. Some of the competent approaches are discussed below:

Marti *et al.,* (2000) proposed a detection approach which makes use of two tools: Watchdog and Path-rater for detecting and mitigating malicious behavior of nodes. Watchdog detects the malicious behaviour of nodes by analyzing the node's behavior based on two levels: the link level and the forwarding level; while, the Path rater uses neutral rating and the suspected rating for identifying misbehaving nodes. Similarly, Buchegger & Boudec, (2002a) contributed a protocol called CONFIDANT, which incorporates four ideal components: the monitor, the reputation system, the path manager and the trust manager. The striking feature of this scheme is the trust manager, which contains updated information about alarms received from the alarm table for detecting maliciousness. This mechanism also incorporates trust table which determines the trust-worthiness of a mobile node and a friend list to which the alarms need to be sent.

Further, Niu *et al*., (2011) proposed a tit-for-tat strategy for punishing the worst behaviour of nodes for enforcing cooperation in the multicast environment based on game theory. Authors also investigated a novel interval based estimation method to resolve the issue of imperfect monitoring of an ad hoc network containing malicious nodes. Buchegger & Boudec, (2002b) proposed a reputation system which maintains a table containing nodes entry as well as its rating. The rating used in this scheme is based on own experience, observation and reported experience of mobile nodes individually. The experiences obtained through direct interaction between mobile nodes are given higher priority when compared to reported experience. Authors used a weight based experience parameter for estimating whether a node is malicious or normal in its routing activity. Michiardi & Molva, (2002) proposed a reputation mechanism for improving the node cooperation level in MANETs. Authors tried to establish a maximum cooperation level between mobile nodes through the use of reputation tables and watchdog. Authors also addressed two issues that differentiate the level of cooperative behavior extended by the mobile nodes.

Furthermore, Wang & Li, (2006) contributed a price based mechanism for identifying rational nodes. A node in this centralized mechanism is assumed to be rational, when it chooses an optimal strategy for relaying a unit of data to their next hop neighbor nodes. Wang *et al*., (2005) proposed a mechanism that could enforce cooperation by isolating selfish nodes based on statistical analysis of data obtained purely through local observation. This mechanism compares the characteristics of neighbour nodes with one another based on online local reputation assessment algorithm.

Yet, Buttyan & Hubaux, (2003) addressed the need of cooperation between the mobile devices for enhancing reliability in an ad hoc environment. The authors assume that mobile nodes are tamper resistant because a tamper resistant node's behavior may not be modified. This mechanism uses a tamper resistant hardware module to mitigate the malicious behavior of the nodes. This methodology has an advantage of using a counter called nuglet counter, which monotonically decreases when a node needs to send the data packets as a source whereas it monotonically increases when a node acts as a router. Kargl *et al*., (2004) proposed a mobile intrusion detection system that possesses the capability of over hearing. In addition, it makes use of sensors for increasing the detection accuracy. This detection system also uses an embedded secured architecture called SAM.

Hortelano *et al.,* (2010) adapted a watchdog sensor and a Bayesian filter for detecting and mitigating malicious behaviour such as black hole attack and selfish mobile nodes in mobile peer to peer networks. A collaborative watchdog mechanism was anticipated by Orallo *et al*., (2012) for detecting selfish nodes in the ad hoc network. They modeled the network with two kinds of mobile nodes: collaborative and selfish nodes. They also formulated a transition probability matrix that stores binary values for computing detection time and total overhead. In their recent work, *Orallo et al*., (2014) incorporated a collaborative watchdog approach for fast dection of selfish nodes. In this work, they also introduced an evaluation model for estimating the time taken for detecting selfish nodes and overhead involved in such detection.

Besides, Mukhtar, (2014) proposed a collaborative contact-based watchdog mechanism which detects the selfish nodes more accurately and in a rapid manner. A token-based umpiring technique was proposed by Kumar *et al*., (2015), that assigns a token for each and every mobile node for participating in the routing activity while the neighboring nodes will act as an umpire for establishing a reliable routing path. Recently, Chiejina *et al.,* (2015) incorporated a first reputation methodology for designing dynamic reputation management system which computed a node's reputation based on which the routing path is established.

In addition, the three benchmark systems utilized for performing comparative analysis with the proposed ERFBM approach are discussed below. The first benchmark

mitigation mechanism used is the Record and Trust-Based Detection (RTBD) contributed by Subramaniyan *et al.,* (2014). This RTBD scheme analyses the detection of selfish nodes through network functions like routing and packet dropping. This mechanism also accelerates the detection of misbehaving nodes and highly reduces the detection time and total overhead. Further, the second benchmark mitigation mechanism used is the Reliability Factor Based Mitigation Mechanism (RFBMM) contributed by Sengathir & Manoharan, (2014). This approach first computes the normalized deficiency factor and then estimates a packet deficiency factor manipulated through the weighted sum of product on the normalized deficiency factor which ensures the reliability of the mobile node through exponential distribution.

Finally, the third benchmark mitigation mechanism utilized for comparison is the Packet Conservation Monitoring Algorithm (PCMA) contributed by Fahad & Askwith, (2006). In this work, authors incorporated a mitigation approach that utilizes dual information obtained from the misbehaving nodes for detecting and isolating them. This monitoring algorithm also works on enhancing the reliable transmission of data and thus increases the overall performance of the network in terms of packet delivery ratio, throughput, total overhead and control overhead by mitigating a special type of malicious node called selfish nodes.

From the survey of the mechanisms proposed in the literature for detecting selfish nodes, it is found to have the following shortcomings.

- A hybrid reputation mechanism that integrates both first and second hand information for identifying selfish nodes based on exponential failure rate has not been explored to the best of our knowledge.
- A mechanism which could forecast the mobile nodes' behavior based on exponential time has not been much explored.

Thus, it is motivated to propose an exponential distribution based isolation mechanism for mitigating selfish nodes. AODV protocol is used as the base protocol for implementing the ERFBM mechanism. Exponential distribution is then used in this approach, since it is highly suitable for estimating reliability and utilizes a single parameter for estimating constant failure rate. Furthermore, exponential distribution highlights the time interval that lies between two independent events that occur at a constant equivalent rate and it is a limiting case of weibull and gamma distributions. This exponential distribution is also memory-less and hence it is highly suitable for investigating the reliable behaviour of mobile node co-operation in packet forwarding.

EXPONENTIAL RELIABILITY FACTOR BASED MITIGATION MODEL (ERFBM)

The ERFBM is formulated to identify the selfish behavior of nodes based on available energy metric and further, to isolate them from the routing path based on ERF by reconfirming the nodes' selfishness for enabling reliable dissemination of data. The problem of isolating selfish nodes can be analyzed in two folds. First, the analysis is based on the available energy of the mobile nodes, which strongly predicts the possibility of a cooperative mobile node to change its behavior into a selfish node. Secondly, reconfirmation of the nodes' selfishness can be estimated based on exponential reliability factor and then decision on isolating them from the routing path is incorporated.

Available energy metric based detection

When a source node wants to send packets to the destination, the ERFBM approach computes the available energy metric (E_m) of each and every mobile node in the routing path. This available energy metric is computed through the ratio of the residual energy (Re_m) to the energy drain rate (Dr_m). Residual energy is the amount of initial energy possessed by the mobile node before data transmission, while the energy drain rate is the rate of energy utilised by the mobile node for participating in the routing activity. Thus, the available energy metric of the mobile node at any time instant 't' is given by Equation (1)

$$E_m = \frac{Re_m}{Dr_m} \tag{1}$$

The drain rate of a mobile node used for calculating available energy metric is manipulated through exponential weighted moving average method given through Equation (2).

$$Dr_m = \alpha \times Dr_k + (1 - \alpha) Dr_{k-1} \tag{2}$$

where, Dr_k and Dr_{k-1} indicate the drain rate of a mobile node in two successive sessions *(Kim, et al. 2003)*. Here, α is defined as the weighted average parameter calculated through the ratio of minimum energy required for transmitting data in a specified routing path to the minimum number of hops existing between the source and destination given by Equation (3)

$$\alpha = \frac{MIN\_Energy\_req}{Min\_Hops} \tag{3}$$

This approach records the energy information by incorporating a table which contains three fields: a) Node identity b) Energy drain rate and c) Available energy metric. When the computed value of available energy metric E_m is found to be less

than the threshold energy E_{th} which is essential for a mobile node to be in cooperative state, then the mobile node is identified as selfish. The value of threshold energy $'E_{th}'$ proposed for our mathematical model is as considered in *Patil, et al. (2011)*. The following algorithm 1 presents the steps involved in the estimation of available energy metric for selfish node detection.

Algorithm 1: Energy based Selfish Node Detection

Notations:

n - Number of mobile nodes in the network

N_m - Represents a node for which E_m to be computed

Re_m - Residual energy of a node Re_m

Dr - Drain rate of a mobile node in a session.

k - Number of sessions

1. for each mobile node $N_m$with Re_m in the network do
2. Compute the drain rate of the N_m using exponential average method through $Dr_m = \alpha \times Dr_k + (1-\alpha)Dr_{k-1}$
3. Compute the available energy of the node using $E_m = \frac{Re_m}{Dr_m}$
4. If $E_m < E_{th}$, then N_m is selfish
5. Call ERF Selfish Node Categorization ( );
6. Else N_m is cooperative.
7. End If
8. End for
9. End.

When a source node S wants to relay packets to a destination node D, it searches for a routing path in its routing table. If the route to the destination node is not found, the source node floods route request RREQ packets to its neighbours. The RREQ packet of ERFBM-AODV is an extension of RREQ packet of AODV protocol, which contains three fields: available energy, residual energy and drain rate. Based on the RREQ packet of ERFBM-AODV, residual energy and drain rate of a mobile is determined for manipulating available energy metric. If the computed available energy metric is less than the energy threshold, then the mobile nodes are identified as selfish and selfish node categorization algorithm is incorporated for classifying the selfish nodes into Type I, Type II and Type III. In contrast, mobile nodes are said to be cooperative when the available energy metric is greater than the energy threshold E_{th}.

The following algorithm demonstrates the steps involved in categorizing the detected selfish nodes.

Algorithm 2: Selfish Node Categorization ( );

Notations:

n - Number of mobile nodes in the network

N_m - Represents a node for which E_m to be computed

Re_m - Residual energy of a node Re_m

Dr_m - Drain rate of a mobile node in a session.

k - Number of sessions

1. for each mobile node N_m with $Re_m \; and \; Dr_m$ in the network do
2. Compute the available energy of the node using $E_m = \frac{Re_m}{Dr_m}$
3. If $(E_m < E_{th1} and \, E_m > E_{th2})$, then

   N_m is designated as Type III selfish node.

   3.1 Begin

   3.2 Call Selfish Rehabilitate( );

   3.3 End
4. Else If $(E_m < E_{th2} \; and \; E_m > E_{th3})$, then N_m is designated as Type I selfish node.

   4.1 Begin

   4.2 Call Exponential Rel_ Factor_Isolate ( );

   4.3 End
5. Else If $(E_m < E_{th3})$, then

   N_m is designated as Type II selfish node.

   5.1 Begin

   5.2 Call Selfish Isolate( );

   5.3 End
6. Else $\mathrm{N_m}$ is cooperative node
7. End If
8. End for
9. End

The selfish node categorization algorithm classifies the selfish nodes based on their available energy levels with respect to three thresholds limits: $E_{th1}(80\ joule), E_{th2}\ (65\ joule)$ and $E_{th3}\ (50\ joules)$ as defined in *Roy & Chaki, (2011b)*. If the value of E_m is found to be less than E_{th1} but greater than E_{th2}, then the node is designated as Type III selfish node and they are isolated from the routing process through Selfish Rehabilitate () function. Similarly, if the value of E_m is found to be less than E_{th2} but greater than E_{th3}, then the node is designated as Type I selfish node. This category of Type I selfish nodes are reconfirmed through Exponential Rel_ Factor_Isolate () function elaborated in algorithm 3. Finally, if the value of E_m is less than E_{th3}, then the node is designated as Type II selfish node and these nodes are mitigated through Selfish Isolate ( ) function which isolates the selfish nodes from the routing path.

Exponential reliability factor based selfish node isolation

When the mobile nodes present in the routing path are identified as Type I selfish node through available energy metric, the decision of isolating them is incorporated through a factor called Exponential Reliability Factor (ERF). This ERF is manipulated through a hybrid reliability computation process that combines both the first hand (direct observation) and second hand (neighbours recommendation) information together.

First hand information based reliability computation

Consider an ad hoc environment that contains mobile nodes identified by a unique id where in 'nr' denotes the number of packets received by a mobile node from their neighbors and 'rp' is the number of packets relayed by that mobile node to the next hop neighbors. Then, the amount of packet drop 'dp' by a node is computed based on the difference between the number of packets received by a node to the number of packets relayed by that node to their neighbors as given by Equation (4)

$$dp = nr - rp \tag{4}$$

If the number of packets dropped by a mobile node in k sessions as identified by their neighbors be $dp_1, dp_2, dp_3, \ldots, dp_k$, then, the average packet drop rate ($APDR_i$) of a mobile node in each session is given by Equation (5)

$$APDR_i = \frac{dp_i}{nr_i}, \tag{5}$$

where, $1 \leq i \leq k$

From the value of $APDR_i$, the primary trust value $'T_p'$ of a mobile node 'm' is calculated based on moving average method through Equation (6)

$$T_P = \sum_{i=1}^{k} \left[\frac{APDR_i \times W_i}{\sum_{i=1}^{k} W_i} \right], \tag{6}$$

where, W_i is the weight factor that quantifies the packet dropping behavior of the monitored mobile node as well as the reliability of the monitoring node in judging a node's cooperation. Further, (W_i) is computed through the variance of the expected average packet drop rate $(APDR_i)$ derived from Equation (5) and is represented through Equation (7)

$$W_i = \sum_{i=1}^{k} \frac{\sum_{i=1}^{k} (APDR_i - APDR_e)}{k-1}, \tag{7}$$

where, $APDR_e$, the average packet drop rate determined for the entire session 'k' is computed through Equation (8)

$$APDR_e = \frac{\sum_{i=1}^{k} APDR_i}{k} \tag{8}$$

Furthermore, the moving average method is incorporated in this reliability computation process since it provides i) stable forecast and ii) high priority for the behavior exhibited by the most recent session as compared to the past session.

Second hand information based reliability computation

This reliability is calculated based on neighbours recommendation about a mobile node through Cohen Kappa statistics, Since it is the well known predominant inter-rater reliability statistic that can be used for recommending a nodes' reputation. Hence, the second hand reliability of a mobile node $'i'$ is determined through the neighbour $'j'$ by Cohen Kappa Reliability Coefficient $(KPRC)$ given through Equation (9),

$$KPRC(i,j) = \frac{P_{obs} - P_{exp}}{1 - P_{exp}}, \tag{9}$$

where,

P_{obs} - represents observed probability of cooperation,

P_{exp} - represents expected probability of cooperation.

Similarly, the recommendation of a mobile node $'i'$ about node $'j'$ is denoted by $KPRC(j,i)$. Then, the secondary reliability (T_s) is computed through Equation (10)

$$T_s = \frac{KPRC(i,j) + KPRC(j,i)}{2} \tag{10}$$

Computation of ERF

The estimation of ERF which reconfirms the selfish behaviour of mobile nodes is done through the computation of Hybrid Reliability Factor (HR_m) which is computed based on the linear combination of primary reliability (T_p) and secondary reliability (T_s) through Equation (11),

$$HR_m = \gamma T_p + (1-\gamma)T_s, \tag{11}$$

where, T_p and T_s lie between 0 and 1 with the constraint $0 \leq \gamma \leq 1$.

Hence, each mobile node in the ad hoc network possesses an HRF through which the reputation of the mobile node is manipulated based on ERF_m given by Equation (12)

$$ERF_m = e^{-HR_m} \tag{12}$$

The following algorithm 3 depicts the steps involved in isolating Type I selfish nodes through exponential reliability factor.

Algorithm 3: Selfish Node Isolation through Exponential Reliability Factor.

Exponential Rel_ Factor_Isolate ( )

n - Number of mobile nodes in the network

P_r - Total number of packets received by a mobile node

P_f - Total number of packets forwarded by a mobile node

N_m - Represents a node for which ERF_m to be computed

W_i - Weight factor that quantifies the packet dropping behaviour

P_{obs} - Observed probability of cooperation,

P_{exp} - Expected probability of cooperation.

// Computation of primary trust factor through first hand information

1. for each mobile node N_m with E_m in the network $m = 1\ to\ n$ do
2. for each and every session $i = 1\ to\ k$ do
3. Compute the number of packet dropped by a mobile node in a session through $dp = nr - rp$
4. Compute the average packet drop rate d_p obtained for each sessions using $APDR_i = \frac{dp_i}{nr_i}$

5. Compute the primary trust value $'T_p'$ through $APDR_i$ for each mobile node using $T_P = \sum_{i=1}^{k} \left[\frac{APDR_i \times W_i}{\sum_{i=1}^{k} W_i}\right]$
6. End for

// Computation of second hand trust factor through second hand information

7. for each neighbour i of a mobile node j in the network $m = 1\ to\ n$ do
8. Compute Cohen Kappa Reliability Coefficient, $KPRC(i,j) = \frac{P_{obs} - P_{exp}}{1 - P_{exp}}$
9. End for
10. for each neighbour j of a mobile node i in the network $m = 1\ to\ n$ do
11. Compute Cohen Kappa Reliability Coefficient, $KPRC(j,i) = \frac{P_{obs} - P_{exp}}{1 - P_{exp}}$
12. Find secondary reliability, $T_s = \frac{KPRC(i,j) + KPRC(j,i)}{2}$
13. End for

//Computation of Hybrid Reliability Factor through primary and secondary realibility

14. for each mobile node N_m in the network $m = 1\ to\ n$ do
15. Manipulate Hybrid Reliability Factor, $HR_m = \gamma T_p + (1 - \gamma) T_s$
16. Compute exponential reliability factor using HR_m through $ERF_m = e^{-HR_m}$
17. If $(ERF_m < 0.40)$ then
18. Call Selfish Rehabilitate ( );
19. Else Enable normal routing activity
20. End If
21. End For
22. End.

Hence, if the ERF for a mobile node is found to be less than 0.4 (as per the simulation conducted and demonstrated in Figure 1), then the node is reconfirmed as selfish and isolated from the routing path. This prediction of selfish nodes could enable the rehabilitation of the entire network so that the performance could be enhanced. The ERF also enables the neighbour nodes to detect selfish nodes in a progressive manner.

SIMULATIONS AND EXPERIMENTAL ANALYSIS

Extensive simulation experiments for ERFBM are carried out through ns-2.26. The simulated network consists of 100 mobile nodes distributed in a terrain size of 1000 x 1000 sq. meters, The packet size, channel capacity and the constant bit rate are considered as 512 bytes, 2 Mbps and 40 packets/sec respectively. It is also assumed that, every mobile node contains 100 joules of energy and that 10 joules of energy is required for each time slot of communication.

The following Table 1 illustrates the simulation parameters setup for our study.

Table 1: Simulation Setup

Parameters	**Values**
No. of Mobile Nodes	100
Terrain area	1000 x 1000 sq. meters
Simulation time	100 seconds
Mobility Model	Random Way point
Traffic Source	Constant Bit Rate (40 packets/sec)
Packet Size	512 Bytes
Protocol	AODV
Propagation Type	Two Ray Ground
Refresh Interval Time	10 seconds
Channel Capacity	2 Mbps

Furthermore, the reliable delivery of data in an ad hoc environment highly depends on the level of cooperation rendered by the intermediate mobile nodes (*Cizeron et al., 2009; Feeney, 2001*) that exists between the source and destination. Hence, the selfish behavior of intermediate mobile nodes decreases the rate of packet delivery and further increases the number of retransmissions (*Li et al., 2009; Wang & L, 2006*). The performance of ERFBM is therefore analyzed using evaluation metrics: packet delivery ratio, throughput, total overhead, control overhead, energy consumption rate and packet latency by varying the number of mobile nodes.

RESULTS AND DISCUSSION

The simulation results represented through Figure 1 demonstrate the comparative analysis carried out for identifying maximum number of selfish nodes by varying threshold range for detection with mitigation mechanisms like ERFBM, RTBD, RFBMM and PCMA.

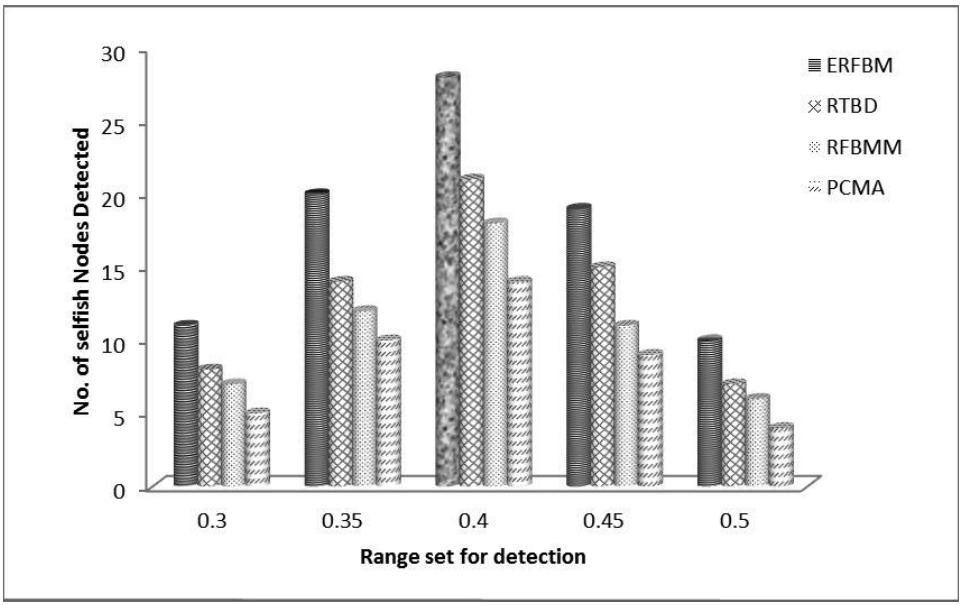


Fig. 1. Determination of Optimal Threshold Point for selfish node detection

In addition, these simulation results also indicate that the proposed ERFBM approach isolates maximum number of selfish nodes than the RTBD, RFBMM and PCMA at 0.4, which is considered as the optimal threshold point of selfish node detection.

Experiment 1 – Performance analysis of ERFBM based on varying number of mobile nodes

In the first experiment, the performance of ERFBM is analysed by varying the number of mobile nodes.In this experiment, 20% of the mobile nodes are considered selfish. The plots of packet delivery ratio, throughput, control overhead and total overhead of experiment-1 are depicted through Figure 2.

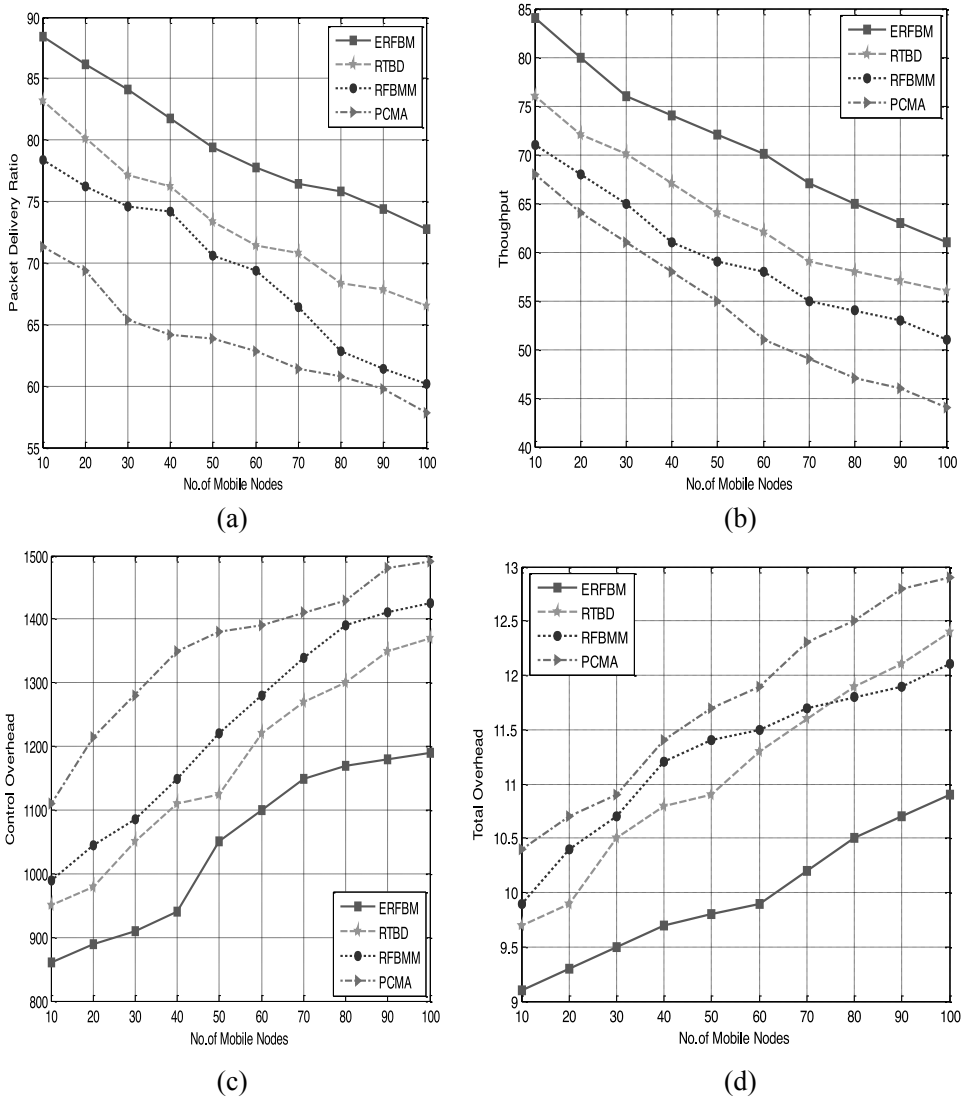


Fig 2: Experiment-1 - Performance Analysis for ERFBM based on (a) Packet Delivery Ratio (b) Throughput (c) Control Overhead (d) Total Overhead

From Figure 2(a), it is observed that, ERFBM increases the packet delivery ratio from 15% - 19% over RTBD, 22% - 26% over RFBMM and from 28% - 33% over PCMA as it isolates maximum number of selfish nodes from the routing path through the computation of exponential reliability coefficient that integrates first and second hand information. Similarly, from Figure 2(b), it is obvious that ERFBM improves the throughput from 12% - 15% over RTBD, 20% - 25% over RFBMM and from 27% - 30% over PCMA.

In contrast, Figure 2(c) and Figure 2(d) demonstrate the performance of ERFBM based on total overhead and control overhead. It is observed that, ERFBM reduces the total overhead from 17% - 11% over RTBD, from 19% - 15% over RFBMM and from 23% - 20% over PCMA, while it reduces the control overhead from 21% - 16% over RTBD, from 28% - 20% over RFBMM and from 36% - 31% over PCMA.

Experiment 2 – Performance Analysis of ERFBM by varying the number of Selfish Nodes with 0.40 as optimal threshold point.

Experiment-2 evaluates the performance of ERFBM over RTBD, RFBMM and PCMA by varying the number of selfish nodes with 0.40 as optimal threshold point for selfish node detection. The plots of packet delivery ratio and throughput for experiment-2 is depicted through Figure 3(a) and Figure 3(b), respectively. From Figure 3(a), it is observed that, ERFBM improves the packet delivery ratio from 13% - 18% over RTBD, 21% - 24% over RFBMM and from 25% - 31% over PCMA. Whereas from Figure 3(b), it is evident that ERFBM increases the throughput from 14% - 18% over RTBD, 22% - 26% over RFBMM and from 24% - 29% over PCMA. Similarly, Figure 3(c) and Figure 3(d) depict the performance of ERFBM based on control overhead and total overhead. It is observed that the ERFBM reduces the control overhead from 27% - 21% over RTBD, from 32% - 29% over RFBMM and from 38% - 33% over PCMA. While at the same time, it reduces the total overhead from 22% - 17% over RTBD, from 27% - 23% over RFBMM and from 34% - 30% over PCMA.

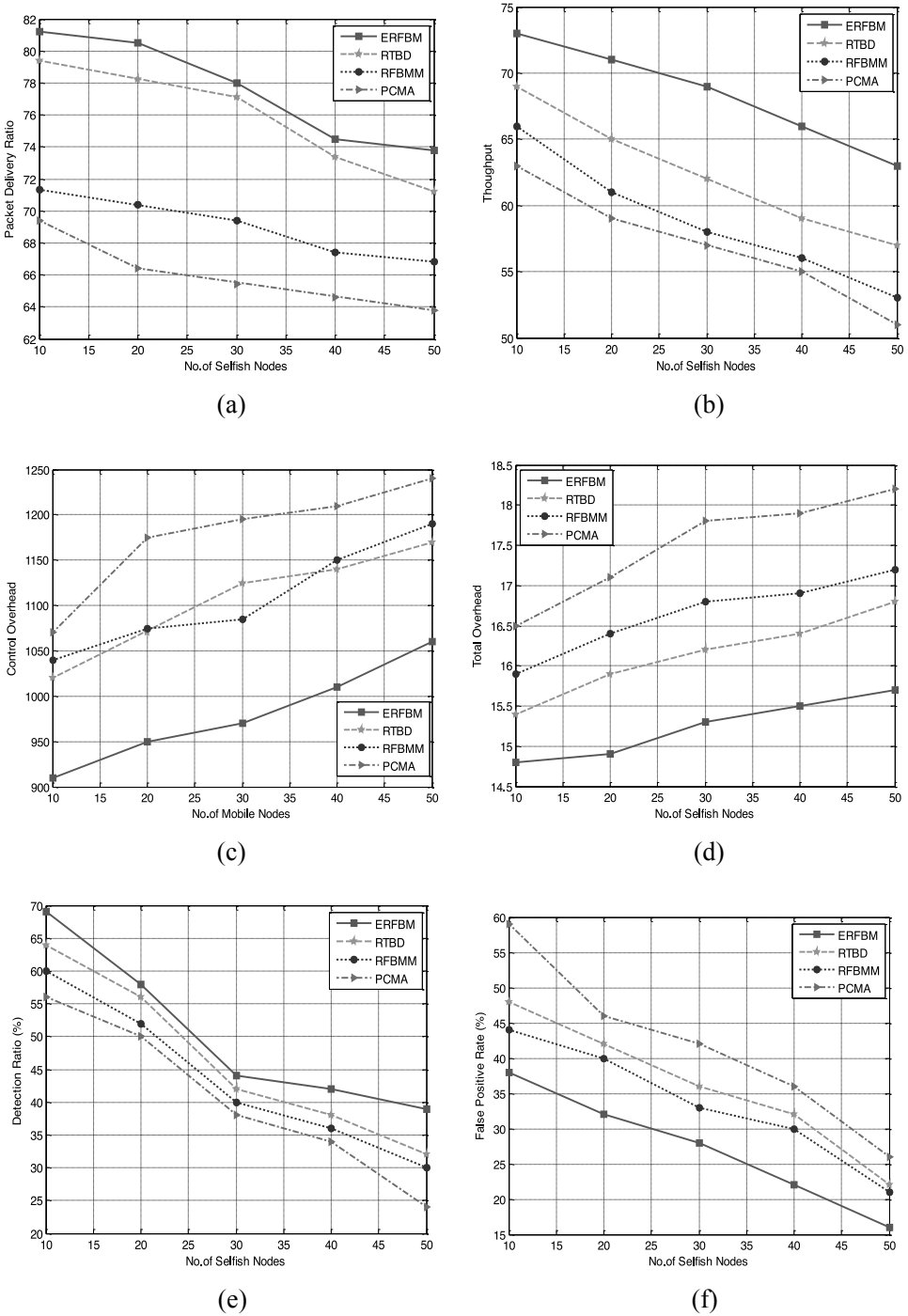
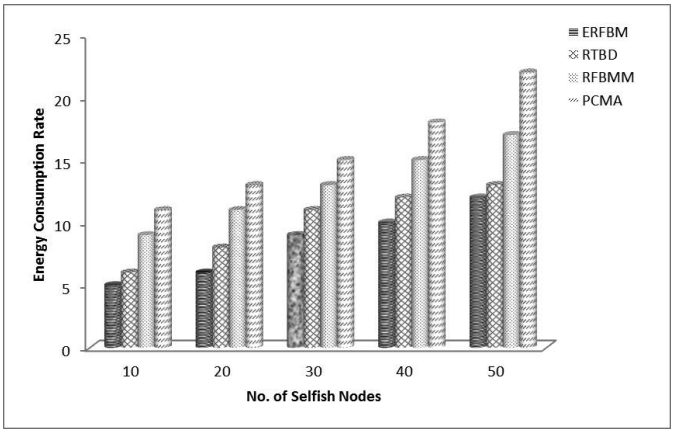


Fig. 3. Experiment-2 - Performance Analysis for ERFBM based on (a) Packet Delivery Ratio (b) Throughput (c) Control Overhead (d) Total Overhead (e) Detection Rate (f) False Positive Rate

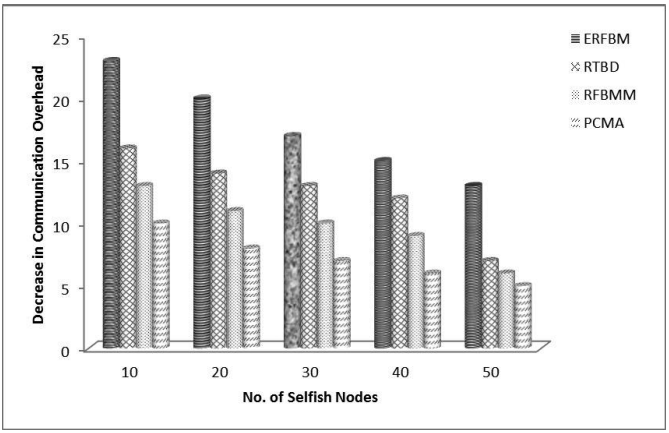
In addition, Figure 3(e) and Figure 3(f) depicts the plots of detection ratio and false positive rate for ERFBM. From Figure 3(e) and Figure 3(f), it is evident that ERFBM detects selfish nodes rapidly at a rate of 23% than RTBD, 28% than RFBMM and 36% over PCMA. Moreover, it reduces the false positive rate from 22% over RTBD, 26% over RFBMM and 32% over PCMA.

Experiment 3 – Performance Analysis of ERFBM based on energy consumption rate and communication overhead

The third experiment evaluates the performance of ERFBM based on percentage decrease in energy consumption rate and communication overhead over RTBD, RFBMM and PCMA by varying the number of selfish nodes. From Figure 4(a), it is clear that ERFBM on an average, decreases the energy consumption rate to a maximum of 23% than RTBD, RFBMM and PCMA.



(a)



(b)

Fig. 4. Experiment-3 - Performance Analysis for ERFBM based on (a) Decrease in Energy Consumption rate (b) Decrease in Communication Overhead

Likewise, It is clear from Figure 4(b) that the proposed ERFBM approach reduces the communication overhead by a maximum rate of 28% than RTBD, RFBMM and PCMA.

CONCLUSION

In this paper, we present an Exponential Reliability Factor based Mitigation Mechanism for detecting and isolating selfish nodes by incorporating both the available energy metric and exponential failure rate of each and every mobile node. The simulation results clearly depict that the proposed ERFBM isolates the selfish nodes at a faster rate and enhances the performance of the network by reducing the control overhead and total overhead from 15% - 22%, 24% - 28% and 29%-34% than RTBD, RFBMM and PCMA, respectively. The proposed ERFBM approach also reduces the energy consumption rate by 23% than the considered benchmark mitigation mechanisms. In addition, this model also aids in framing a threshold value of 0.40 as the optimal threshold point for selfish node detection. In the near future, we are planning to evaluate the performance of ERFBM approach by varying the energy level and traffic load under different optimal threshold point set for selfish node detection.

REFERENCES

Amir Khusru, Akhtar & Sahoo, G., 2009. Mathematical Model for the Detection of Selfish Nodes in MANETs," International Journal of Computer Science and Informatics, 1(3): 25-28.

Azni, A.H., Ahmad, R., Noh Z. A. M., Basari, A. S. H & Hussin, B., 2012. Correlated Node Behavior Model based on Semi Markov Process for MANETS. IJCSI International Journal of Computer Science, 9(1): 50-59.

Buchegger, S & Boudec, J-Y., 2002a. 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, 226-236.

Buchegger, S & Boudec, J-Y., 2002b. Nodes bearing Grudges: Towards routing security, Fairness, and Robustness in Mobile Ad-Hoc Networks. in Proc., Tenth Euro micro workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, 403-410.

Buttyan, L & Hubaux, J-P., 2003. Stimulating Cooperation in Self–organizing Mobile Ad hoc Networks," MONET Journal of Mobile Computing and Networking: 8(1): 579-592.

Campos, C.A.V & de Moraes, L.F.M., 2011. A Markovian Model Representation of Individual Mobility Scenarios in Ad Hoc Networks and Its Evaluation. EURASIP Journal on Wireless Communications and Networking, 3(1): 231 –5292.

Cizeron, E., & Hamma, S., 2009. Multipath routing in MANETs using Multiple Description Coding. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 282 – 287.

Chiejina, E., Xiao, H., & Christianson, B., 2015. A Dynamic Reputation Management System for Mobile Ad Hoc Networks. Computers, 4(1): 87-112.

Fahad, T. & Askwith, R., 2006. A Node Misbehavior Detection Mechanism for Mobile Ad hoc Networks. in Proc., Seventh Annual Post Graduate Symposium on the convergence of Telecommunications,

Networking and Broadcasting (PGNet), 78-84.

Feeney. L. M., 2001. An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks. ACM Journal of Mobile Networks and Applications, 6(3): 239–249.

Hortelano, J., Carlos T., Calafate, D., Cano, J. C., de Leoni, M, Manzoni, P., & Mecella, M., 2010. Black-Hole Attacks in P2P Mobile Networks Discovered through Bayesian Filters. OTM 2010 Workshops, LNCS 6428, 543–552,

Kargl, F., Klenk, S., Schlott & Weber, M., 2004. Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks. in Proc., First European Workshop on Security in Ad-Hoc and Sensor Network (ESAS 2004), Heidelberg, Germany, 255-263.

Kim, D. J. J., Aceves, G. L & Obraczka, K., 2003. Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate. IEEE Transactions on Mobile Computing, 2(2): 161-173.

Kumar, J. M. S., Karthivel. A., Kirubakara. N., Sivaraman. P. & Subramanian. M, 2015, A Unified Approach for Detecting and Eliminating Selfish Nodes in MANETs using TBUT. Eurasip Journal on Wireless Communications and Networking, 1(3) : 143-154.

Kumar. K. A., & Bahadhur, S., 2013. Selfish Node Detection in Replica Allocation over MANETs. IOSR Journal of Computer Engineering (IOSR-JCE), 13(5): 7-13.

Li, Z., Jia, Z, Zhang, R & Wang. H., 2009. Trust-based on-demand multipath routing in mobile ad hoc networks, Special Issue on Multi Agents and Distributed Information Security, IET Information Security, 4(4): 212-232.

Li, Z & Shen, H., 2012. Game-theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Network. IEEE Transactions on Mobile Computing 11(8), 1287-1303.

Marti, S., Giuli, T, J., Lai, K & Baker, M., 2000. Mitigating routing misbehavior in mobile ad hoc networks. in Proc., 6th ACM Annual International Conference on Mobile Computing and Network (ACM-MobiCom), Boston, USA, 255-265.

Michiardi. P & Molva. R, 2002, CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. in Proc., 6th IFIP Conf. on Security, Communications and Multimedia, Protoroz, Solvenia, 107-121.

Mukhtar, M. K., 2014. A Collaborative Contact-based Watch dog for detecting Selfish Nodes in Cooperative MANETs. An International Journal of Research in Engineering and Technology, 3(11): 437-442.

Niu, B. H., Zhao, V & Jiang, H., 2011. A Cooperation Stimulation Strategy in Wireless Multicast Networks," IEEE Transactions on Signal Processing, 59(5): 2355-2369.

Orallo, H, E., Manuel D., Olmos, S., Cano, J., C., & **Calafate & Manzoni, T., 2012.** Improving Selfish Node Detection in MANETs Using a collaborative Watchdog. IEEE Communication Letters, 16(5): 642-645.

Orallo, H, E., Manuel D., Olmos, S., Cano, J., C., & Manzoni, P., 2014. A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs. Wireless Personal Communications, 74(3): 1099-1116.

Patil, P. A., Kanth, B. S. R., Kumar, M. P. D & Malavika. J. 2011. Design of Energy Efficient Routing protocols for MANETs. International Journal of Computer Science, 8(1): 215-220.

Pusphalatha, M., Revathy, V & Rama Rao, P., 2009. Trust based Energy aware reliable reactive protocol in mobile ad hoc networks. World Academy of Science, Engineering and Technology, 3(27): 335-338.

Roy, D. P., & Chaki, R., 2011a. Detection of Denial of Service Attack Due to Selfish Nodes in MANET

by Mobile Agent, CCIS 162, Springer Verlag pp. 14-23.

Roy, D. P., & Chaki, R., 2011b. MADSN Mobile Agent Based Detection of Selfish Node in MANET. International Journal of Wireless & Mobile Network, 3(4), 225-235.

Sengathir, J & Manoharan, R., 2014 A reliability factor based mathematical model for isolating selfishness in MANETs', International Journal of Information and Communication Technology, 6(3/4): 403-421.

Subramaniyan, S., Johnson. W & Subramaniyan, K., 2014 A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) Technique. EURASIP Journal on Wireless Communications and Networking, 1(1): 205-211.

Wang, B., Soltani, S., Shapiro, J. K & Tan, P. K., 2005. Local Detection of Selfish Routing Behavior in Ad hoc Networks. in Proc., 8th IEEE International Conference on Parallel Architectures, Algorithms and Networks, 1(1): 16-22.

Wang, W & Li, X. Y., 2006. Low-Cost Routing in Selfish and Rational Wireless Ad Hoc Networks," IEEE Transactions on Mobile Computing, 5(5), pp. 596-607.

Submitted: 16/3/2015

Revised: 10/7/2015

Accepted: 12/7/2015