Wireless Personal Communications (2019) 108:1493–1511
https://doi.org/10.1007/s11277-019-06481-0

A Hyper-Exponential Factor-Based Semi-Markov Prediction Mechanism for Selfish Rendezvous Nodes in MANETs

Sengathir Janakiraman[1] · Bipin Bihari Jayasingh[1]

Published online: 6 May 2019

Abstract

In multi-hop wireless network like mobile ad hoc network (MANET), co-operation between mobile nodes under group communication is inevitable for ensuring reliable network connectivity as they lack a centralized point of control. In such multicasting network, rendezvous point acts as a trusted intermediary and plays a vital role of relaying packets between the downstream and upstream nodes for ensuring reliable data dissemination. The selfish misbehaviour of core group leader node degrades the performance of the network by intentionally dropping a significant amount of packets. Most of the existing mitigation techniques contributed for handling rendezvous point misbehaviour relies on watchdog, path rater and Bayesian filter for detection as they are capable in elucidating past evidences. But these detection components face certain limitations in quantifying the reputation of mobile nodes. In this paper, hyper-exponential factor-based semi-Markov prediction mechanism (HEFSPM) is formulated for estimating the likely probability of mobile nodes that has the possibility of being compromised by rendezvous point misbehaviour. HEFSPM uses a Semi-Markov process for forecasting the probability as the failure rendezvous point node cannot be rehabilitated into a co-operative node Further, Semi-Markov is highly efficient when they quantify the reputation value of nodes based on their anticipated future behaviours. Simulation results portray that HEFSPM is predominant in handling rendezvous point misbehaviour and improves packet delivery ratio and throughput by 24% and 22% superior to the considered baseline mitigation approaches. An analytical validation of HEFSPM is also performed using the Rayleigh distribution for proving its efficacy in forecasting nodes' misbehaviour.

Keywords Selfish rendezvous nodes · Core group leader · Multicasting · Network survivability · Semi-Markov prediction mechanism

✉ Sengathir Janakiraman
j.sengathir@gmail.com

Bipin Bihari Jayasingh
bbjayasingh9@rediffmail.com

[1] Department of IT, CVR College of Engineering, Mangalpally, Ibrahimpatnam, Telangana 603319, India

1 Introduction

The term ‘Network survivability’ refers to the expected degree of potential rendered by network in sustaining its reliable services under the impact of malicious behaviours and random failures. Network survivability is considered as the most significant entity to be ensured as the multicasting ad hoc networks are highly susceptible to network partition. Specifically, the transition of rendezvous point core group leader from its co-operative state to selfishly acting malicious state drastically influences the survivability of the network [1]. Further, network connectivity is used as the significant quantification metric for evaluating the survivability of the network by a number of diversified works in the literature [2]. In addition, majority of the mitigation mechanisms proposed in the literature handles rendezvous point misbehaviour by computing the reputation value either by quantifying information related to the past history or by estimating the conditional probability factor of the mobile nodes [3–5]. However, these mitigation techniques are not potentially capable of detecting rendezvous point misbehaviour by forecasting each participating mobile node’s behaviour using likelihood probability of behavioural transition computed based on its present characteristics [6]. Thus the behaviour of each participating mobile node needs to be forecasted and further network survivability has to be quantified using network connectivity for maintaining a resilient environment among the mobile nodes [7–15].

Further, Sengathir and Manoharan [16] contributed a Futuristic Trust Coefficient-Based Semi-Markov Prediction (FTCSPM) mechanism that forecasts the mobile node’s likelihood probability of possible behavioural transitions. The likelihood probability of mobile nodes quantifies the magnitude of possibility that induce them to alternate from one behavioural state to another. This magnitude of possibility is estimated based on stochastic properties collected from the mobile nodes. FTCSPM emphasizes that a failed mobile node can never be rehabilitated into a selfish node. Hence, FTCBSMP utilizes a special kind of Markov chain called non birth–death process by ignoring the restriction of the nearest neighbour-based behavioural transitions of mobile nodes. Moreover, the Markov chain utilized in FTCSPM mainly analyses the co-operative, selfish and failure state of mobile nodes. Finally, Authors [17] proposed a trust and energy integrated future behaviour forecasting mechanisms known as Hyper-geometric Trust Factor based Markov Prediction Mechanism (HTFMPM). This Hyper-geometric factor based forecasting technique forecasts the likelihood probability of a multicast shared tree group leader being infected by rendezvous point misbehaviour. HTFMPM relies on a Hyper-geometric integrated factor that uses a Markov prediction process for analyzing the possible behavioural transitions of shared tree group leader under multicasting. The results of HTFMPM prove its remarkable performance in terms of packet drop rate, average end-to-end delay and energy consumptions. HTFMPM is analytically validated based on the Weibull distribution for emphasizing its effectiveness in predicting rendezvous point misbehaviour.

From the literature reviewed, the following shortcomings are identified and listed below:

(a) The majority of the existing Semi-Markov process-based rendezvous point misbehaviour forecasting mechanism has not used a non birth–death process with an exponential parameter for prediction.

(b) A prediction mechanism that models service and repair events based on exponential distribution and two-phase hyper-exponential distribution for mitigating rendezvous point misbehaviour for ensuring maximum network survivability has not been investigated.

The aforementioned limitations induces us to formulate an Hyper-Exponential Factor-based Semi-Markov Prediction Mechanism (HEFSPM) for effective and efficient mitigation of selfishly behaving rendezvous point nodes.

In this paper, Hyper-Exponential Factor-based Semi-Markov Prediction Mechanism (HEFSPM) is proposed for forecasting the mobile node's likelihood probability of possible behavioural transitions. The likelihood probability of mobile nodes defines the magnitude of possibility that induce them to alternate from one behavioural state to another. This magnitude of possibility is estimated based on the stochastic properties collected from the mobile nodes. In addition, HEFSPM mechanism emphasizes that a failed rendezvous point core leader can never be rehabilitated into a selfishly acting rendezvous point node. Hence, HEFSPM utilizes a special kind of Markov chain called non birth–death process by ignoring the restriction of the nearest neighbour-based behavioural transitions of mobile nodes. Moreover, the Markov chain utilized in HEFSPM mainly analyses the co-operative, compromised rendezvous point and failure state of mobile nodes under multicasting.

The remaining sections of the paper are structured as follows. Section 2 depicts an Hyper-Exponential Factor-based Semi-Markov Prediction Mechanism that helps in the futuristic behavioural prediction of mobile nodes under multicasting. Section 3 portrays the analytical validation of HEFSPM using Rayleigh distribution. Section 4 highlights on the simulation setup used for implementing HEFSPM with the comparative investigation carried out with the considered baseline mitigation schemes. Section 5 concludes by highlighting the major contributions and future enhancements feasible from this research.

2 Hyper-Exponential Factor-Based Semi-Markov Prediction Mechanism (HEFSPM)

HEFSPM is an efficient Semi-Markov forecasting mechanism proposed for effectively identifying and isolating rendezvous point misbehaviour through the computation of futuristic probability. Futuristic probability quantifies the possibility or chance of a root node mobile node being compromised by malicious behaviour. HEFSPM is a distributed approach that investigates the behaviour of each shared tree root node or rendezvous point node for maliciousness.

In HEFSPM, failure time and repair time of each mobile node follows exponentially distribution and two-phase hyper-exponential distribution respectively. Hence the life time of each mobile node based on repair time distribution is

$$L_{f(t)} = \lambda_1 \mu_1 e^{-\mu_1 t} + \lambda_2 \mu_2 e^{-\mu_2 t} \tag{1}$$

Let 'm' be the possible states of each mobile node and its state space is denoted as (0, 1, 2, 3,…, m). The stochastic process of HEFSPM follows Semi-Markov as the transition of each mobile node behaviour depends on the present state and to some extent on the past history.

The states of HEFSPMis denoted using two tuples (i, j), where i and j represents the initial and final state of transition of each participating mobile node. Based on the possible behaviour of mobile node, the complete set of states of HEFSPM is

(i) $P(0,0)$—The probability of the mobile node to exhibit co-operative behaviour without any misbehavior.

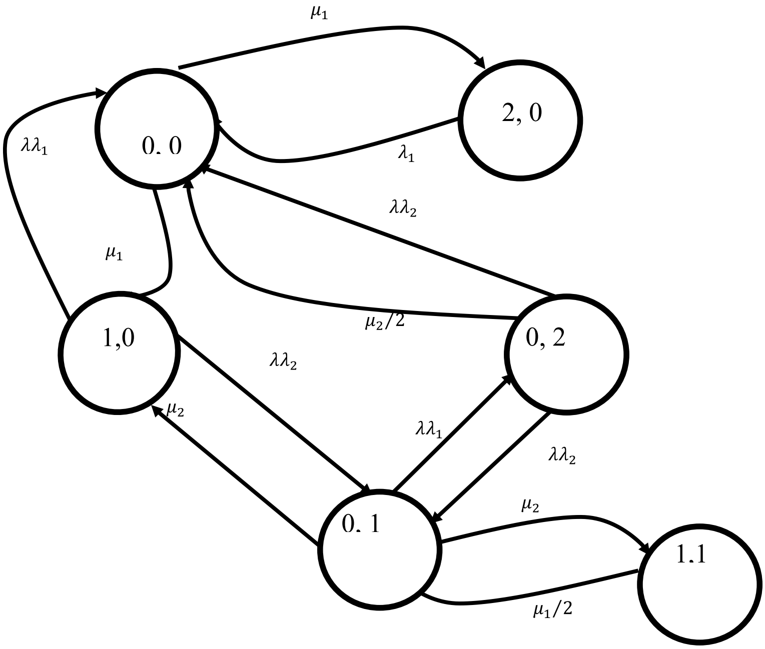

Fig. 1 Transition diagram of HEFSPM

(ii) $P(1,0)$—The probability of the mobile node to get transited from selfish rendezvous point misbehavior to co-operative behaviour

(iii) $P(0,1)$—The probability of mobile node to get transited from co-operative behaviour to selfish rendezvous point misbehavior.

(iv) $P(2,0)$—The probability of mobile node to get transited from selfish and network pruning induced rendezvous point misbehaviour to co-operative behaviour

(v) $P(1,1)$—The probability of mobile node to get retained in selfish rendezvous point misbehaviour

(vi) $P(0,2)$—The probability of mobile node to get transited from co-operative behaviour to selfish and network pruning induced rendezvous point misbehaviour.

From transition diagram depicted in Fig. 1, the balance equations of HEFSPM are derived as

$$\lambda P(0,0) = \mu_1 P(1,0) + \mu_2 P(0,1) \tag{2}$$

$$(\mu_1 + \lambda)P(1,0) = \mu_1 P(2,0) + \lambda_1 P(0,0) + \frac{\mu_2}{2}P(1,1) \tag{3}$$

$$(\mu_2 + \lambda)P(0,1) = \mu_2 P(0,2) + \lambda_2 P(0,0) + \frac{\mu_1}{2}P(1,1) \tag{4}$$

$$\mu_1 P(2,0) = \lambda\lambda_1 P(1,0) \tag{5}$$

$$\mu_2 P(0,2) = \lambda\lambda_2 P(0,1) \tag{6}$$

$$\left(\frac{\mu_1 + \mu_2}{2}\right)P(1,1) = \lambda\lambda_1 P(0,1) + \lambda\lambda_2 P(1,0) \tag{7}$$

Further, the parametric solution of the above equations in terms of $P(0,0)$ are derived as

$$P(1,0) = \frac{\lambda\lambda_1}{\mu_1}P(0,0) \tag{8}$$

$$P(0,1) = \frac{\lambda\lambda_2}{\mu_2}P(0,0) \tag{9}$$

$$P(0,2) = \left(\frac{\lambda\lambda_2}{\mu_2}\right)^2 P(0,0) \tag{10}$$

$$P(2,0) = \left(\frac{\lambda\lambda_1}{\mu_1}\right)^2 P(0,0) \tag{11}$$

$$P(1,1) = \frac{\lambda^2\lambda_1\lambda_2}{\mu_1\mu_2}P(0,0) \tag{12}$$

The probability of mobile node under its normal behaviour P(0, 0) is computed based on the normalization condition given by

$$P(0,0) + P(1,0) + P(0,1) + P(2,0) + P(0,2) + P(1,1) = 1 \tag{13}$$

Further the reduced description probability of mobile node in co-operative state P(0,0) is

$$P(0) = P(0,0) \tag{14}$$

Furthermore the reduced description of HEFSPMin terms of P(1) that combines P(1,0) and P(0,1) that represents the mobile in either selfish or network pruning induced rendezvous point misbehavior is

$$P(1) = P(1,0) + P(0,1) \tag{15}$$

In addition, the reduced description of HEFSPM in terms of P(2) that combines P(2,0), P(0,2) and P(1,1) that represents the mobile node in selfish or network pruning induced rendezvous point misbehavior or in exhibiting both the kinds of rendezvous point misbehavior is

$$P(2) = P(2,0) + P(0,2) + P(1,1) \tag{16}$$

Hence, from the derived parametric equations, the aforementioned probabilities P(1) and P(2) calculated using P(0) from equation in order to forecast the type of root node misbehavior at any instant of time is

$$P(1) = \lambda\left(\frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2}\right)P(0) \tag{17}$$

$$P(2) = \lambda^2\left(\frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2}\right)^2 P(0) \tag{18}$$

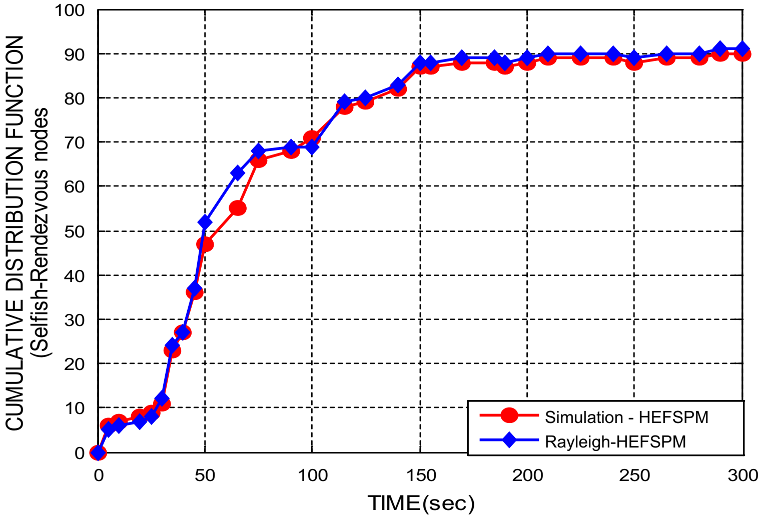

Fig. 2 Analytical validation of HEFSPM through Rayleigh distribution

From the forecasted value of P(1) and P(2) that represents the mobile node in selfish or network pruning induced rendezvous point misbehavior or in exhibiting both the kinds of rendezvous point misbehavior, the decision of mitigation of root node attack is initiated when the forecasting threshold is below 0.35 based on [18].

3 Validation of HEFSPM Mechanism

HEFSPM prediction scheme is validated through analytical and simulation experiments by calculating the cumulative density function of rendezvous point misbehaviour nodes. HEFSPMis analytically validated using Rayleigh distribution as it is the predominant probabilistic distribution which is potential in investigating the lifetime of mobile nodes using probability density function. Analytical investigation of HEFSPM proves that it requires an average transition time of 6.49 s for being compromised by rendezvous point misbehaviour from its co-operative state. Figure 2 depicts that analytical validation using Rayleigh distribution is highly correlated with the simulation results.

Moreover, HEFSPM defines the rendezvous point misbehaviour survivability rate as the observed proportion of mobile nodes identified as selfish to the probable number of mobile nodes that has the inductive probability of being compromised. HEFSPM in an average possesses a rendezvous point misbehaviour survivability rate of 34% in withstanding the network connectivitymore than FTCSPM, ECNBM, CNBM and PBM approaches considered forcomparative study. The analytical results of HEFSPM also prove that rendezvous behaviour of mobile nodes iswell identified between the maximum and minimum detection time of 110 and 130 s respectively.

4 Simulation Experiments and Results Analysis

The performance of HEFSPM is thoroughly studied using network simulator ns-2.32. The main objective of this simulation investigation is to prove the correctness of the proposed HEFSPM. The performance of HEFSPMis then compared with the selfish rendezvous point misbehaviour forecasting mechanisms like FTCSPM, ECNBM, CNBM and PBM. The comparative performance of HEFSPMis carried out using performance metrics such as PDR, throughput, energy consumption, average end-to-end delay and packet drop rate [19–22].

4.1 Simulation Environment

HEFSPM is implemented in the simulated environment that consists of 100 mobile nodes that randomly move around the terrain area of 1000 × 1000 meters to portray the influence of small and large networks. Further, simulations are carried out using random way-point model with the CBR traffic rate and simulation time of 50 packets per second and 300 s respectively.

4.2 Results and Discussions

HEFSPMis evaluated using three experiments by varying (a) the number of mobile nodes, (b) the number of selfish rendezvous point nodes and (c) the number of CBR traffic flows.

(a) Experiment 1—Performance investigation of HEFSPM observed by varying the number of mobile nodes

In experiment-1, HEFSPMis analyzed by varying the mobile nodes of the network in which 20% of them are set as selfish rendezvous point misbehaviour nodes.

Figures 3 and 4 depict the results of PDR and throughput of HEFSPM. In general, PDR and throughput of the network decreases proportionally when the number of active mobile nodes increases. This decrease is mainly because of the impact of extra number of packets forced to be relayed by the network. However, HEFSPM mechanism considerably increases the PDR and throughput by utilizing a trust-based rendezvous point misbehaviour nodes forecasting mechanism that investigates the behavioural change of mobile nodes. Hence, HEFSPM increases the PDR value by 9–12% over FTCSPM, 14–17% over ECNBM, 19–21% over CNBM and 22–25% over PBM. Similarly, HEFSPM shows an increase in throughput by 4–6% over FTCSPM, 7–11% over ECNBM, 13–16% over CNBM and 18–21% over PBM.

Thus HEFSPM exhibits an increased mean performance of 14.5% and 17.2% superior to the baseline mitigation schemes with respect to PDR and throughput.

Similarly, Figs. 5 and 6 demonstrate the results of energy consumptions and average end-to-end delay of HEFSPM. The energy consumption rate and end-to-end delay of HEFSPM increases when the numbers of packet need to be forwarded by the mobile nodes increases. But HEFSPM decreases the energy consumptions and end-to-end delay

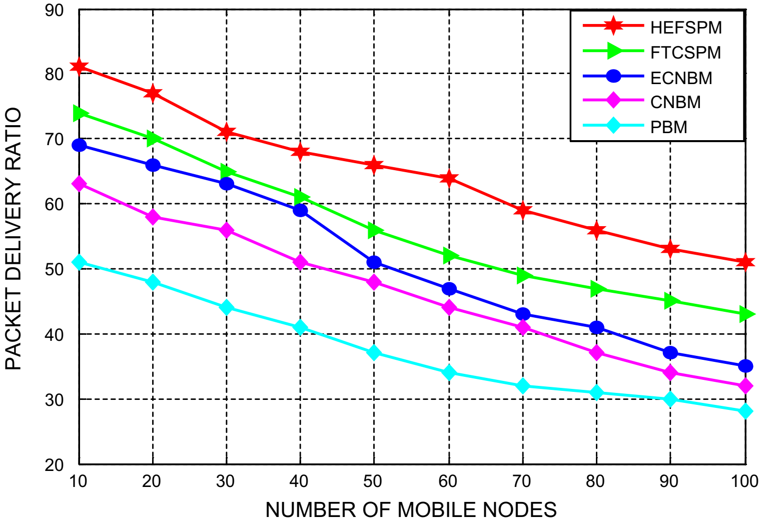

Fig. 3 Experiment 1—packet delivery ratio

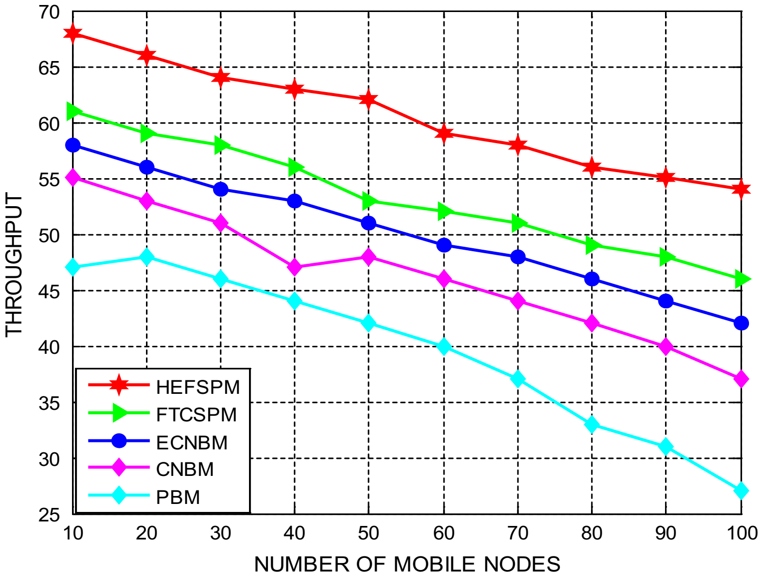

Fig. 4 Experiment 1—Throughput

by accurately predicting the possible nodes' behavioural changes for maintaining network connectivity.

Hence, HEFSPM decreases the energy consumptions by 5–7% over FTCSPM, 9–11% over ECNBM, 13–16% over CNBM and 18–22% over PBM. HEFSPM also decreases average end to end delay from 7 to 9% over FTCSPM, 10–12% over ECNBM, 14–16%

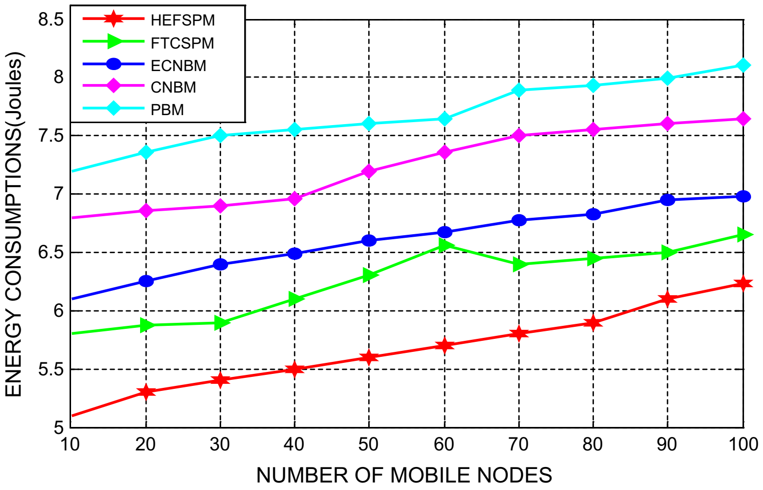

Fig. 5 Experiment 1—energy consumption

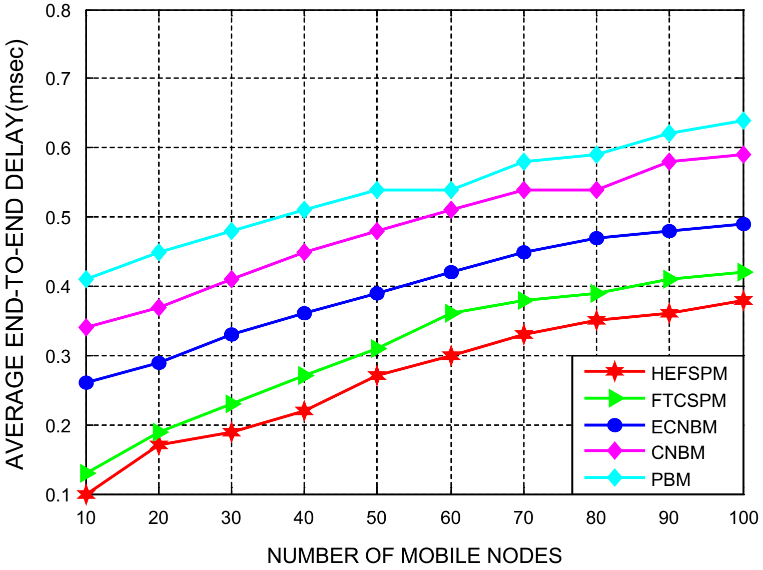

Fig. 6 Experiment 1—average end-to-end delay

over CNBM and 19–22% over PBM. Thus HEFSPM on an average decreases the energy consumptions and average end-to-end delay by 13.8% and 15.4% superior to the baseline future forecasting mechanisms considered for study.

In addition, HEFSPM is also investigated based on the packet drop rate as shown in Fig. 7. The packet drop rates of HEFSPM, FTCSPM, ECNBM, CNBM and PBM drastically increase when the mobile nodes are forced to forward additional number of packets than generally transmitted. However, HEFSPM reduces the packet drop rate by analyzing

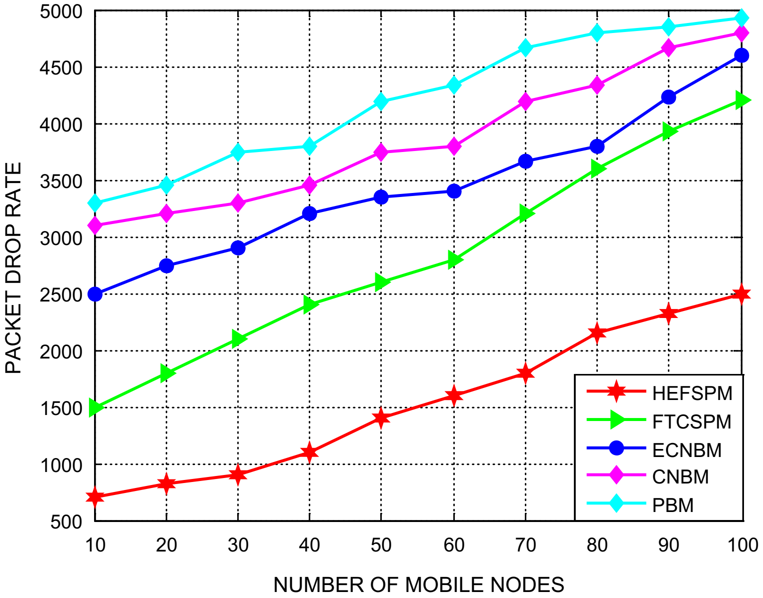

Fig. 7 Experiment 1—packet drop rate

the possibility of reliable packet forwarding process through future forecasting. Hence, HEFSPM shows a phenomenal decrease of packet drop rate by 7–9% over FTCSPM, 10–15% over ECNBM, 17–21% over CNBM and 21–29% over PBM. Thus, HEFSPM on an average decreases packet drop rate by 22.6% greater than the compared futuristic misbehaviour mitigation approaches.

(b) Experiment 2—Performance investigation of HEFSPM observed by varying the selfish rendezvous point nodes

In experiment 2, the performance of HEFSPM is compared with FTCSPM, ECNBM, CNBM and PBM by varying the number of selfish rendezvous point nodes of the multicast network. Figures 8 and 9 highlight the results of PDR and throughput of HEFSPM, FTCSPM, ECNBM, CNBM and PBM which decrease with increase in the number of rendezvous point misbehaviour nodes. But HEFSPM is efficient in isolating the rendezvous point misbehaviour nodes by estimating the likelihood possibility of rendezvous point misbehaviour. Hence, HEFSPM increases PDR by 6–9% over FTCSPM, 11–14% over ECNBM, 17–21% over CNBM and 24–26% over PBM. HEFSPM also improves the throughput by 8–10% over FTCSPM, 11–14% over ECNBM, 15–19% over CNBM and 20–23% over PBM. Thus HEFSPM demonstrates an improvement in PDR and throughput by 20.8% and 17.6% respectively.

Figures 10 and 11 portray the results of energy consumptions and average end-to-end delay of HEFSPM, FTCSPM, ECNBM, CNBM and PBM. The energy consumptions and average end-to-end delay increases as the number of rendezvous point misbehaviour nodes increases in the network. But, HEFSPM conserves energy to a considerable level and establishes reliable links in order to decrease the average end-to-end delay of packets. Further, HEFSPM reduces energy consumptions by 10–13% over FTCSPM, 14–19% over

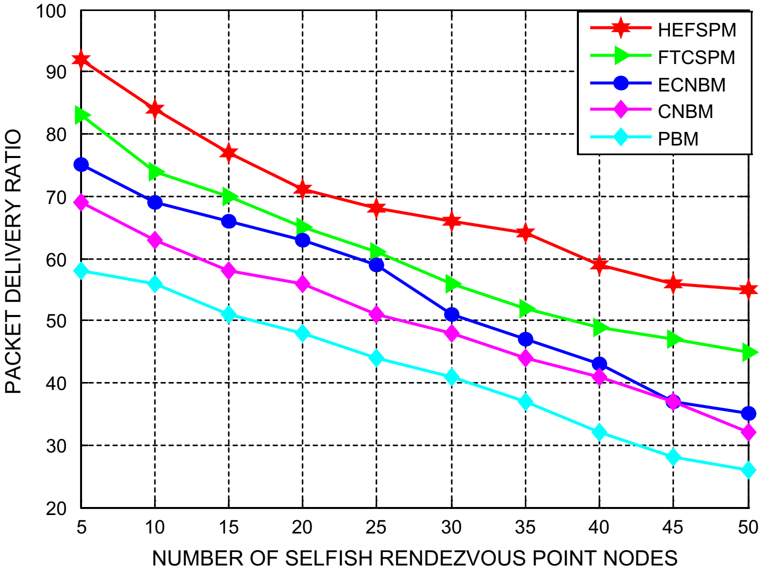

Fig. 8 Experiment 2—packet delivery ratio

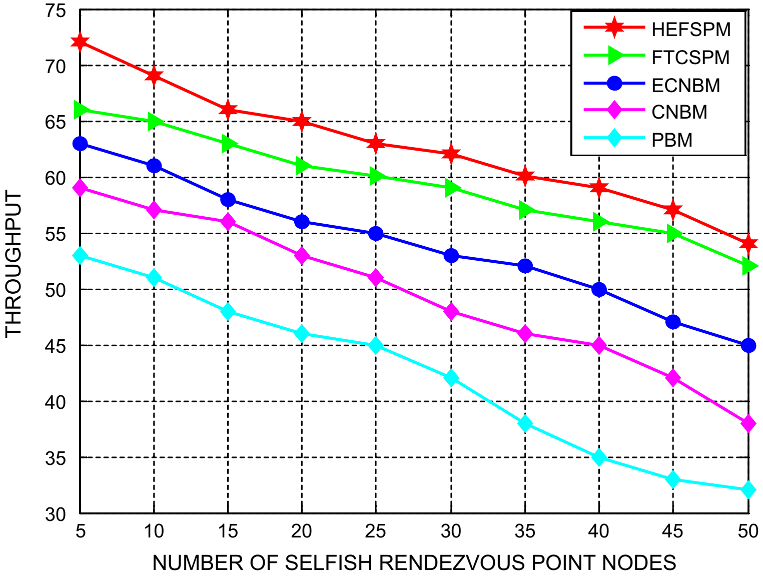

Fig. 9 Experiment 2—throughput

ECNBM, 19–22% over CNBM and 24–28% over PBM. Further, it also minimizes the average end to end delay by 5–8% over FTCSPM, 8–15% over ECNBM, 18–22% over CNBM and 23–28% over PBM. Hence, HEFSPM on an average decreases the energy consumptions and average end-to-end delay by 19.2% and 21.8% respectively.

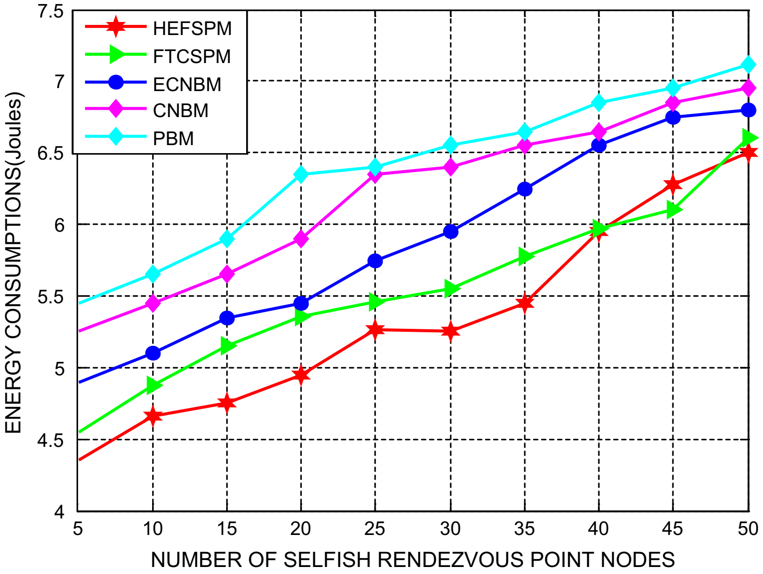

Fig. 10 Experiment 2—energy consumptions

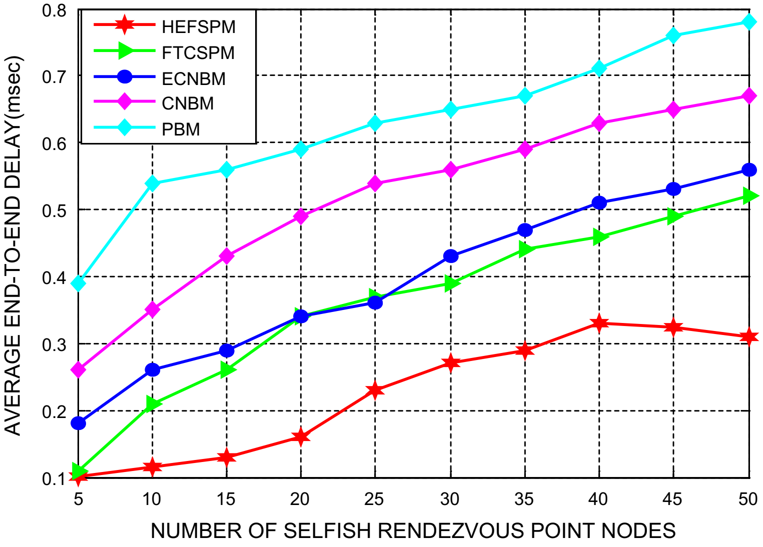

Fig. 11 Experiment 2—average end-to-end delay

Similarly, Fig. 12 depicts the results of packet drop rate which increases when the number of rendezvous point misbehaviour nodes drop maximum number of packets rather than forwarding them. But HEFSPM reduces the packet drop by isolating rendezvous point misbehaviour nodes at a rapid rate of 36% greater than the baseline future forecasting approaches considered for study. HEFSPM decreases the packet drop rate by 8–10% over

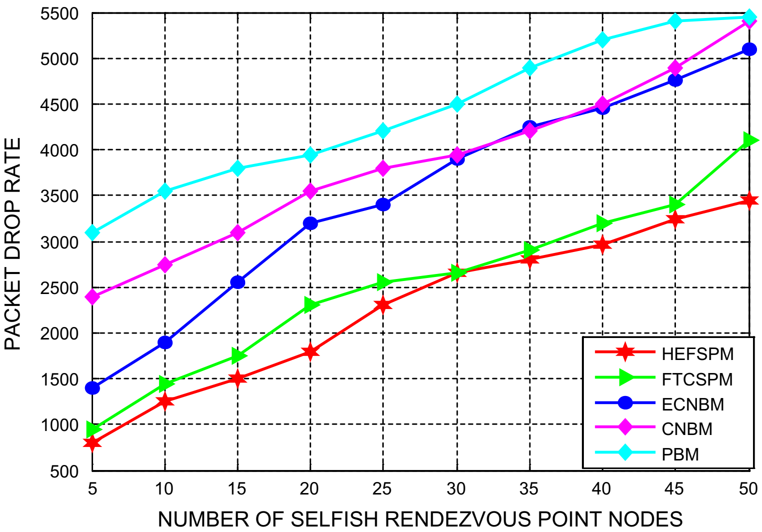

Fig. 12 Experiment 2—packet drop rate

FTCSPM, 10–17% over ECNBM, 19–23% over CNBM and 25–28% over PBM. In addition, it also decreases the packet drop rate on an average by 19.8% greater than the three existing mitigation mechanisms used for investigation.

(c) Experiment 3—Performance investigation of HEFSPM for varying number of traffic flows

In experiment 3, HEFSPM approach is compared with the benchmark systems by varying the number of traffic flows of the network. Figures 13 and 14 depict that PDR and throughput decrease with increase in the number of traffic flows. However, HEFSPM shows a considerable improvement in PDR and throughput by dynamically adjusting the number of packets forwarded. Hence, HEFSPM exhibits an improvement in PDR by 12–14% over FTCSPM, 16–22% over ECNBM, 24–26% over CNBM and 27–29% over PBM. It also shows an improvement in throughput by 11–13% over FTCSPM, 14–17% over ECNBM, 18–23% over CNBM and 25–28% over PBM. Thus, HEFSPM on an average increases the PDR and throughput by 16.8% and 17.4% respectively.

Similarly, Figs. 15 and 16 highlight the performance of energy consumptions and average end-to-end delay by varying the number of traffic flows. The energy consumptions and average end-to-end delay considerably increases linearly with respect to systematic increase in traffic flow rate. But HEFSPM shows significant improvement in the energy consumed even when there are high traffic flows. Hence, HEFSPM decreases energy consumptions by 14–17% over FTCSPM, 21–23% over ECNBM, 23–28% over CNBM and 30–33% over PBM. HEFSPM also exhibits a decrease in the average end-to-end delay to a maximum extent of 7–10% over FTCSPM, 11–14% over ECNBM, 15–21% over CNBM and 17–25% over PBM. Thus HTFMPM on an average minimizes the energy consumptions and average end-to-end delay from 21.8 to 22.6% and 16.6–17.8% respectively.

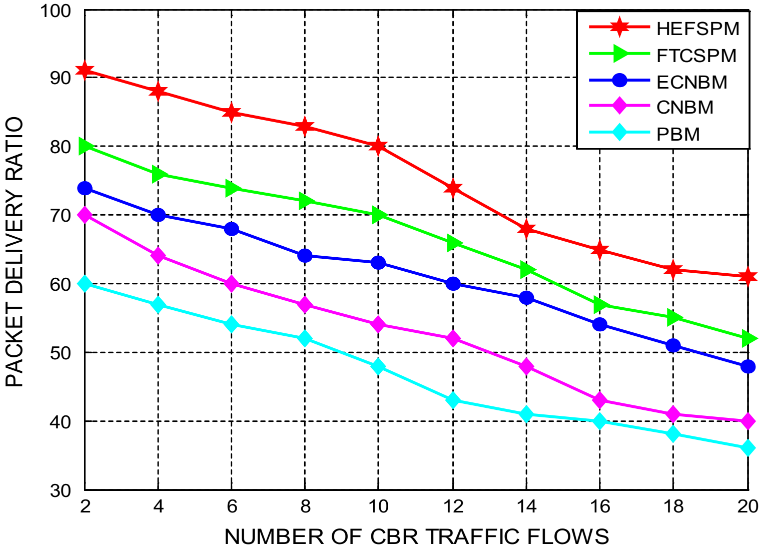

Fig. 13 Experiment 3—packet delivery ratio

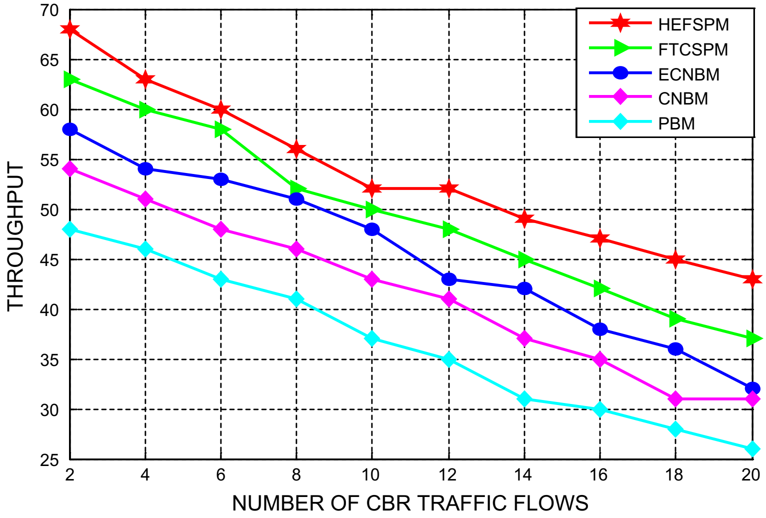

Fig. 14 Experiment 3—throughput

Figure 17 depicts packet drop rate exhibited by HEFSPM when the number of CBR traffic flows are varied. The packet drop rate of HEFSPM decreases systematically with increase in the number of CBR traffic flow. However, HEFSPM is efficient enough in normalizing data packets with corresponding increase in the incoming number of packets to be forwarded by each individual node. Hence it decreases the packet drop rate to an extent of 4–7% over FTCSPM, 8–13% over ECNBM, 17–21% over CNBM and 25–28% over PBM.

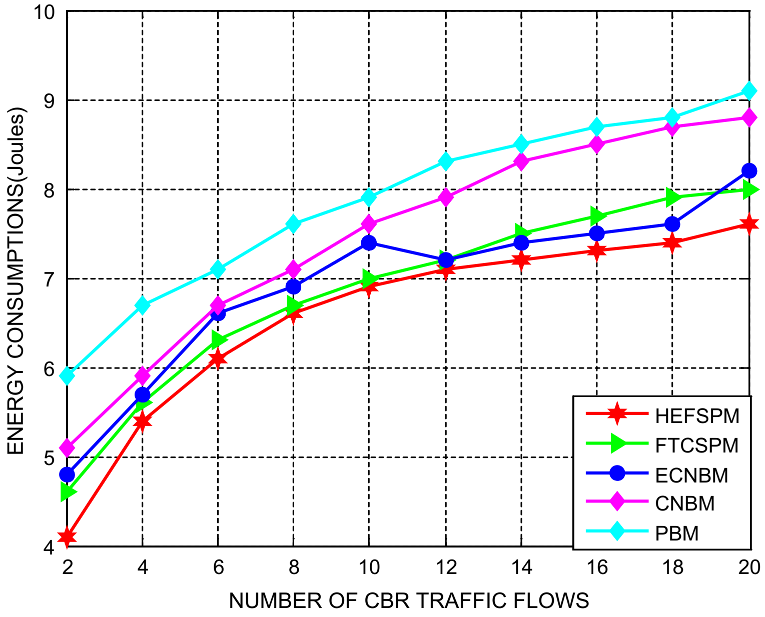

Fig. 15 Experiment 3—energy consumptions

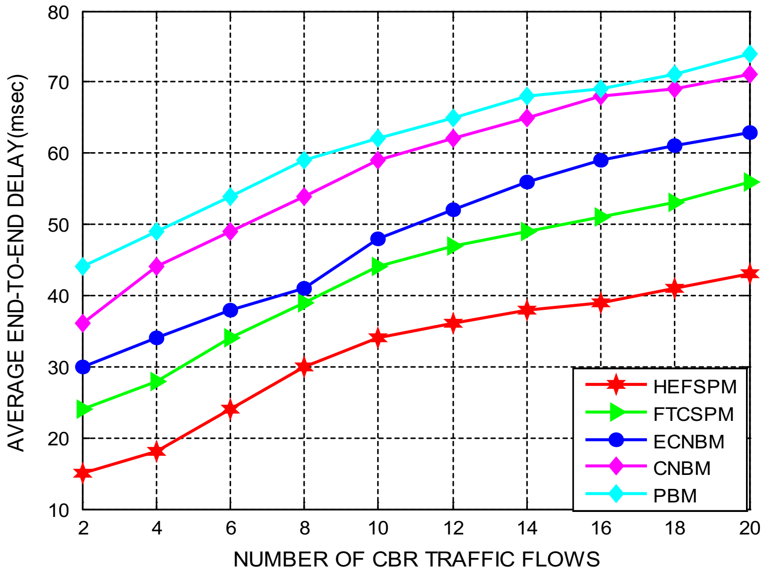

Fig. 16 Experiment 3—average end-to-end delay

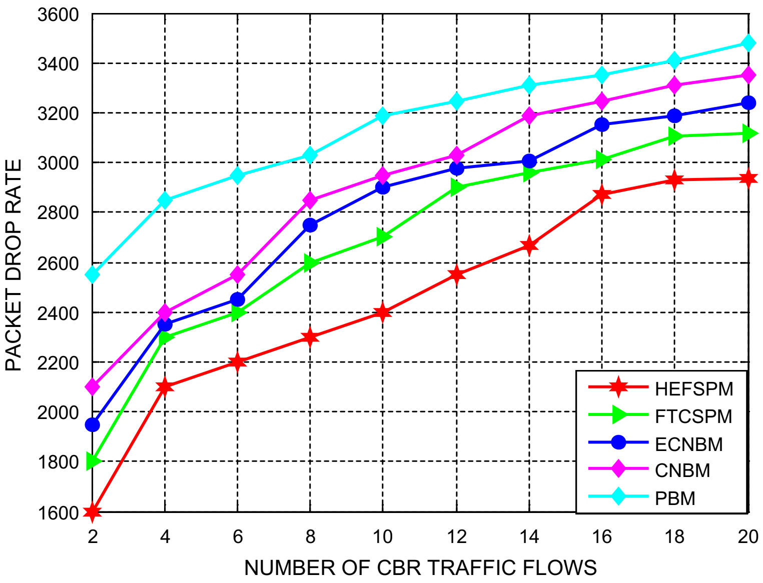

Fig. 17 Experiment 3—packet drop rate

It is also proved that HEFSPM is phenomenal in reducing the packet drop rate in an average by 18.5% superior to the baseline mitigation approaches considered for investigation.

In addition, the comparative analysis of HEFSPM with FTCSPM, ECNBM, CNBM and PBM is performed by varying the number of mobile nodes, selfish rendezvous point nodes and CBR traffic flows based on control overhead and total overhead. HEFSPM found to minimize the control overhead to a maximum level of 18%, 21%, 25% and 24% with respect to FTCSPM, ECNBM, CNBM and PBM mitigation mechanisms. HEFSPM is found to reduce the total overhead by 12%. 15%, 18% and 24% when compared to FTCSPM, ECNBM, CNBM and PBM mitigation schemes.

Finally, the performance of HEFSPM is also compared with HTFMPM by varying the number of mobile nodes, selfish rendezvous point nodes and CBR traffic flows based on throughput, total overhead and packet drop rate. When mobile nodes are varied, HTFMPM exhibits an average improvement in throughput by 15% and they reduce the total overhead and packet drop rate by 17% and 21% with respect to HEFSPM. Similarly, when number of selfish rendezvous nodes are varied, HTFMPM is found to maximize the throughput by 16% than HEFSPM and they are also found to reduce the total overhead and packet drop rate by 14% and 18% with respect to HEFSPM. The performance improvement of HEFSPM based on CBR traffic flow with respect to FTCSPM, ECNBM, CNBM and PBM is summarized in Table 1.

5 Conclusion

This paper has unveiled and detailed the significance of Hyper-Exponential Factor-based Semi-Markov Prediction Mechanism that isolates selfish rendezvous point misbehaviour by computing futuristic trust probability-based non birth–death process-based exponential

Table 1 Summary of results of HEFSPM based on CBR Traffic flow

Selfish Rendezvous node mitigation mechanism	Increase in PDR (%)	Decrease in total overhead (%)	Decrease in control overhead (%)	Decrease in packet drop rate (%)
HEFSPM	14.6	18.6	19.4	21.6
FTCSPM	12.4	15.6	17.3	19.8
ECNBM	11.4	13.4	15.2	16.4
CNBM	9.4	12.5	12.6	14.2
PBM	7.6	10.8	10.6	11.2

factor. HEFSPM is analyzed through analytical validation using Rayleigh distribution and the simulation results are analyzed based on packet delivery ratio, throughput, energy consumption rate, average end-to-end delay and packet drop rate. Simulation results confirm that HEFSPM enhances throughput and packet delivery ratio 18.6% and 20.8% respectively. HEFSPM reduces packet drop rate, energy consumptions and average end-to-end delay to a maximum extent of 20.4%, 24% and 26% than the baseline mitigation mechanisms considered for study. In addition, HEFSPM facilitates a rapid detection rate of 36% superior to the baseline mitigation schemes considered for investigation. But this detection rate is comparatively 4% lower than HTFMPM. The analytical results of HEFSPM validated using Rayleigh distribution confirm that the obtained simulation results are highly correlated to the analytical results. A Poisson modulated Semi-Markov process has been planed to be used for investigating the mitigation of rendezvous point misbehaviour in the near future.

References

1. Md. Akhtar, A. K., & Sahoo, G. (2008). Mathematical model for the detection of selfish nodes in MANETs. *International Journal of Computer science and Informatics, 1*(3), 25–28.
2. Buchegger, S., & Boudec, J.-Y. (2002). *Nodes bearing Grudges: Towards routing security, fairness and robustness in mobile ad-hoc network*. Presented at tenth Eurominicro workshop on parallel, distributed and network based processing, Canary Islands, Spain.
3. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *Mobile Computing and Networking, 1*(1), 255–265.
4. 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.
5. Tang, J., Cheng, Y., & Zhuang, W. (2011). An analytical approach to real-time misbehavior detection in IEEE 802.11 based wireless networks. In *Proceedings of 30th IEEE international conference on computer communications, joint conference of the IEEE computer and communications societies, Shanghai, China* (Vol 1, No. 1, pp. 1638–1646).
6. Jaggi, N., Giri, V. R., & Namboodiri, V. (2011). Distributed reaction mechanisms to prevent selfish misbehavior in wireless ad hoc networks. In *Proceedings of the global communications conference, GLOBECOM 2011, Houston, Texas, USA* (Vol. 1, No. 1, pp. 1–6). IEEE.
7. Xing, F., & Wang, W. (2006). Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes. In *Proceedings of IEEE international conference on communications* (Vol. 4, No. 3, pp. 1879–1884).
8. Vallam, R. D., Franklin, A. A., & Murthy. C. S. R. (2008). Modelling co-operative MAC layer misbehaviour in IEEE 802.11 ad hoc networks with heterogeneous loads. In *Proceedings of 6th international*

symposium on modeling and optimization in mobile, ad hoc, and wireless networks and workshops, WIOPT Berlin, Germany (Vol. 1, No. 1, pp. 197–206).

9. Komathy, K., & Narayanasamy, P. (2007). A probabilistic behavioral model for selfish neighbors in a wireless ad hoc network. *International Journal of Computer Science and Network Security, 7*(7), 77–82.
10. Xing, Fie. (2009). *Modeling, design, and analysis on the resilience of large-scale wireless multi-hop networks*. Raleigh, NC: Department Of Engineering, North Carolina State University.
11. Cárdenas, A. A., Radosavac, S., & Baras, J. S. (2009). Evaluation of detection algorithms for MAC layer misbehavior: Theory and experiments. *IEEE Transactions on Networking, 17*(2), 605–617.
12. Xing, F., & Wang, W. (2010). On the survivability of wireless ad hoc networks with node misbehaviors and failures. *IEEE Transactions on Dependable and Secure Computing, 7*(3), 284–299.
13. Hernandez-Orallo, E., Serraty, M. D., Cano, J.-C., Calafate, T., & Manzoni, P. (2012). Improving selfish node detection in MANETs using a collaborative watchdog. *IEEE Letters, 16*(5), 642–645.
14. Azni, A. H., Ahmad, R., Noh, Z. A. M., Basari, A. S. H., & Hussin, B. (2013). Correlated node behavior model based on semi Markov process for MANETS. *International Journal of Computer Science Issues, 9*(1), 25–32.
15. Azni, A. H., Ahmad, R., Noh, Z. A. M., Basari, A. S. H., & Hussin, B. (2013). Epidermic modelling for correlated node behavior in ad hoc networks. *International Journal of Chaotic Computing, 1*(1), 22–30.
16. Sengathir, J., & Manoharan, R. (2015). A futuristic trust coefficient-based Semi-Markov prediction model for mitigating selfish nodes in MANETs. *EURASIP Journal on Wireless Communications and Networking, 1*(1), 23–29.
17. Shandilya, V., Simmons, C. B., & Shiva. S. (2014). Use of attack graphs in security systems. *Journal of Computer Networks and Communications*, *2014*(1), 1–13.
18. Patil, A. P., Kanth, K. R., Sharanya, B., Kumar, M. P. D., & Malavika, J. (2013). Design of energy efficient routing protocol for MANETs based on AODV. *IJCSI, 8*(1), 215–220.
19. Tang, J., Jiang, B., Chang, C.-C., & Luo, B. (2013). Corrigendum to "Graph structure analysis based on complex network". *Digital Signal Processing, 23*(4), 713–725.
20. Guang, L., Assi, C. M., & Benslimane, A. (2008). Enhancing IEEE 802.11 random backoff in selfish environments. *IEEE Transactions on Vehicular Technology, 57*(3), 1806–1822.
21. Sundarajan, T., & Shanmugam, A. (2010). Modeling the behavior of selfish forwarding nodes to simulate cooperation in MANET. *International Journal, 2*(2), 147–160.
22. Manohar, P., Vereshechaka, M., & Manjanth, D. (2010). Survivability analysis under non-uniform stochastically dependent node damages. *National Conference on Communications, 1*(1), 1–5.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. Sengathir Janakiraman is currently working as an Associate Professor in the Department of Information Technology from CVR College of Engineering, Mangalpally, Telangana, India. He has received his B.Tech. degree in Computer Science and Engineering, M.Tech. degree in Information security and Ph.D. degree in Mobile ad hoc Networks from Pondicherry Engineering College, Pondicherry, India. He is the recipient of the Pondicherry University Gold Medal in the year 2010. He has more than 12 years of teaching experience in the teaching subjects of Automata Languages and Computation, Information Security and Compiler Design. His fields of interest include Mobile Ad hoc Networks and Software Engineering.

Dr. Bipin Bihari Jayasingh M.Tech, Ph.D. in Comp. Sci., Professor at CVR College of Engineering, Ibrahimpatan(M), Hyderabad, RR Dist-501510, India. He has published 59 research papers in various national/international conferences and journals. He is an awardee of Junior Research Fellow (JRF) of Directorate of Forensic Science, Govt. of India. He has been nominated for young scientist award in the Indian Science Congress Association (ISCA 2006), held in Acharya N.G. Ranga Agriculture University, Hyderabad, Jan. 3–7, 2006. At present, he is guiding 7 Ph.D students. His research interest is on Network security, Intrusion detection Systems, Cybercrime and forensics, multi agent systems, Big data and IOT.