Wireless Pers Commun (2017) 97:3427–3447
DOI 10.1007/s11277-017-4677-2

Co-operation Enforcing Reputation-Based Detection Techniques and Frameworks for Handling Selfish Node Behaviour in MANETs: A Review

J. Sengathir[1] · **R. Manoharan**[1]

Published online: 31 July 2017

Abstract In Mobile Ad hoc Network, co-operation between mobile nodes is inevitable for enabling reliable network connectivity due to the absence of pre-deployed infrastructure. In such a network, mobile nodes spend significant amount of energy for detecting routes and forwarding packets in order to enforce co-operation. The energy drain of mobile nodes due to the above fact induces them to refuse forwarding of packets for their neighbouring nodes in order to participate in the network. The mobile nodes that forward their own packets but drop the packets received from neighbours are known as selfish nodes. Detecting selfish nodes is one of the most challenging issues that need to be addressed for enforcing co-operation. The core objective of this research work is to essentially identify and highlights various reputation-based selfish node mitigation approaches available in the literature with their merits and limitations. This paper presents context-aware reputation-based selfish node mitigation approaches that are classified into three categories viz., History-based reputation mechanism, Condition probability-based reputation mechanism and Futuristic probability-based reputation mechanism. This paper further presents a review on a number of selfish node mitigation frameworks and also aims in emphasizing the role of statistical reliability co-efficient that could aid in effective and efficient mitigation of selfish nodes.

Keywords Selfish nodes · Reputation · History-based reputation · Condition probability-based reputation · Futuristic probability-based reputation · Statistical reliability co-efficient

✉ J. Sengathir
j.sengathir@gmail.com

R. Manoharan
rmanoharan@gmail.com

[1] Department of Computer Science and Engineering, Pondicherry Engineering College, Pillaichavady, Puducherry, India

1 Introduction

From the past decade, diversified research techniques were proposed for mitigating selfish nodes. These mitigation mechanisms mainly focus on enhancing the degree of co-operation between the mobile nodes even during the event of failures and attacks. The selfish node mitigation approaches existing in the literature are broadly categorized into six different classes, viz., (i) Incentive-based detection techniques, (ii) Token-based detection techniques, (iii) Secured routing techniques (iv) Acknowledgement-based detection techniques, (v) Mobile agent-based detection techniques and (vi) Reputation-based detection techniques. Among those techniques, Reputation-based mitigation approaches clearly distinguish the mobile nodes of the network into co-operative and misbehaving by manipulating the reputation factor [1]. This reputation factor is defined as the extent of trust, a node has obtained for itself by interacting or behaving with other nodes. In other words, reputation is a measure of subjective probability with which a mobile node assesses another mobile node or a group of mobile nodes that could exhibit a quantifiable action and exposable in a context that affects the mobile node's action. Moreover, the introduction of probability theory portrays on the premise that "Reputation is better viewed as a threshold point, located on any probability distribution scale of observations and expectations". This reputation can take a range of values that lie between 0 and 1 or any scale of convenience based on the context of application [2]. The reputation value of 1 and 0 represents the genuineness and non-co-operative behaviour of mobile nodes respectively. Further, reputation factor estimated between mobile nodes are measurable and predictable. Furthermore, based on the end-users' behavioural reputation, the trust-based models allow deciding reliability and cooperativeness of a node. The nodes that have high reputation or trust value are provided with services whereas the nodes with low reputation or trust value are isolated from the network. Reputation scheme does not require centralized entity like virtual bank or tamper proof hardware for a node. Instead a distributed mechanism can be implemented for increasing the scalability in MANET. In this paper, a thorough review of possible context-aware reputation mechanisms and frameworks for mitigating selfish nodes are detailed with a special emphasis on their merits and limitations.

The remaining part of the paper is organized as follows. Section 2 provides an eagle view on the definition of selfish behaviour of mobile nodes with their causes, impacts and categorization. Section 3 details on the three possible context-aware reputation mechanisms and frameworks that are contributed in the literature for mitigating selfish nodes in order to enhance the resilience of the network. Section 4 elaborates on the role of statistical reliability co-efficient that are suitable for quantifying reputation of mobile nodes in any context-aware situation and application. Section 5 unveils possible challenging issues of concern that has to analyzed for implementing effective context-aware mitigation techniques and frameworks for selfish nodes. Section 6 concludes the review with some initiatives and scope for future research.

2 Selfish Node Behaviour

The mobile nodes that exhibit selfish behaviour intentionally delay and drop packets when the packets are relayed between the source and destination nodes. Selfish nodes do not support any packet forwarding activity that could benefit their neighbouring nodes. The selfish node also utilizes limited energy for its own purpose with the objective of saving its

resources to a maximum extent. In addition, this misbehaviour is specifically observed only when the residual energy possessed by the mobile nodes is inadequate [3]. Thus a selfish node refuses to participate in the routing process and poses a negative impact on reliability, fairness and efficiency in packet forwarding. Further, the selfish nodes are classified into TYPE I, TYPE II and TYPE III selfish nodes. TYPE I selfish nodes actively co-operate in the route establishment process but intentionally deny to forward data packets for their neighbours regardless of its energy resources. While TYPE II selfish nodes neither co-operate in route establishment nor in data transmission. Whereas TYPE III selfish nodes co-operate in route establishment but do not forward data packets because of its limited availability of residual energy.

2.1 Impacts of Selfish Behaviour

The selfish behaviour of mobile nodes in an ad hoc network induces the following impacts [4].

i. *Network partitioning* The selfish behaviour of mobile nodes ends up with network partitioning. This network partitioning is considered as a serious problem in a dynamic network like MANET. Since the intermediate mobile nodes that forward the desirable data may get isolated and results in reduced data accessibility among the active mobile nodes.

ii. *Reduced data availability* The selfish node behaviour of mobile nodes results in the loss of certain number of mobile nodes and breakage of wireless links that originate a number of disjoint partitions in the network. The mobile node in one disjoint partition hinders the data accessibility of other mobile nodes present in other partitions of the network.

iii. *Decrease in network lifetime* Network lifetime generally refers to the time-span during which the network operates actively prior to the cease of its actions. Since the selfish nodes do not participate in transmitting the packets and also it drains considerable amount of energy. This typical behaviour of selfish nodes drastically decreases the lifetime of the network.

iv. *Decrease in throughput* Selfish behaviour of mobile nodes induce them to drop packets intentionally. Hence, the throughput that denotes the number of packets forwarded by the mobile node for the sake of their neighbours gets degraded.

v. *Increase in packet dropping rate* The selfish nodes drop the maximum number of packets that are received from their neighbouring nodes for conserving its limited energy. This increases the packet drop rate which results in communication overhead in the network.

In the next section, context-aware reputation-based selfish nodes mitigation Techniques is reviewed for reducing the impact of the aforementioned impacts.

3 Context-Aware Reputation-Based Selfish Nodes Mitigation Techniques

Reputation-based selfish node mitigation approaches are classified into three types based on the information gathered and utilized for mitigation. They are first hand information based approaches, second hand information based approaches and hybrid reputation information based techniques. In first hand reputation approach, the mobile nodes' behaviour is monitored by direct interaction collected from one-hop distant mobile nodes and this method of gathering information contributes to local reputation factor. Second hand

reputation approaches on the other hand identifies node behaviour based on the information obtained from the neighbors of the monitored node. In other words, indirect reputation (second hand information) aids in elucidating the reputation information about a mobile node from its neighboring nodes of the network [5]. Finally, hybrid reputation mechanisms is an efficient and effective reputation mechanism that provides reliable information about a mobile node based on cumulative events as monitored by direct and indirect (through neighbors) interactions [6]. These hybrid approaches are identified as highly efficient and effective as they utilize local and global reputation values for selfish node mitigation.

Further, based on the context of behaviour monitoring, these reputation-based selfish node mitigation approaches are also classified into three categories, viz., (i) History-based reputation mechanism, (ii) Condition probability-based reputation mechanism and (iii) Futuristic probability-based reputation mechanism as portrayed in Fig. 1.

3.1 History-Based Reputation Mechanisms

The history-based reputation mechanism mitigates selfish behaviour of the mobile nodes by quantifying their reputation factor based on the past behaviour. Initially, Marti et al. [7] proposed a watchdog-based trust model that listens to every activity of the neighboring node's communication in a promiscuous mode of operation. This competent reputation framework identifies misbehaving nodes based on two levels of rating known as suspected rating and neutral rating. These rating levels are estimated based on watchdog and path rater mechanisms. The core idea behind this reputation framework lies in the isolation of non co-operating malicious nodes from the routing activity rather than punishing them. Figure 2 illustrates the concept involved in watchdog monitoring mechanism that identifies the selfish and malicious activities in MANET.

For instance, the source node 'S' wants to send packets to its destination 'D', though a reliable routing path formed by the intermediate nodes, 'A', 'B' and 'C' (as shown in Fig. 2). According to the watchdog monitoring mechanism, the node 'A' overhears the conversations performed by node 'B'. A Collaborative REputation (CORE) scheme was implemented by Michiardi and Molva [8] with watchdog as the monitoring component. This watchdog component aids in monitoring all the neighboring nodes of every mobile node in the network. The node behaviour in terms of packet forwarding rate and packet receiving rate are analyzed by monitoring. Based on these factors, the reputation values of the mobile nodes are estimated. The estimated reputation value of a mobile node is compared with the threshold value (expected value) of reputation to identify its malicious behaviour. A node possessing a reputation value less than the threshold is identified as selfish and isolated from the routing path. In CORE mechanism, the value of reputation factor of a node ranges from positive to negative values. This range of values shows that

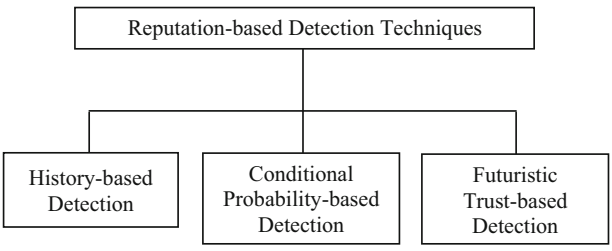

Fig. 1 Types of reputation-based detection techniques

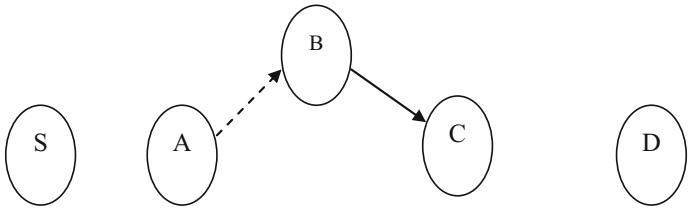

Fig. 2 Watchdog mechanism

this mechanism provides rewards for the well behaving nodes and at the same time punishes the malicious nodes. The main drawback of this mechanism lies in the manipulation of reputation factor determined only from the past history of mobile nodes. But a mobile node with good historical behaviour may also turn into selfish due to resource constraints. They also categorize reputations levels for detecting selfish nodes into three types, viz., (i) subjective reputation, (ii) functional reputation and (iii) indirect reputation. Subjective reputation method computes the reputation value by assigning priority to previous observation of mobile nodes rather than present observation. Using the watchdog scheme, a node's subjective reputation value is altered when a malicious node is identified while indirect reputation assigns a reputation value to another node. Based on the reply message, the list of co-operative nodes is updated based on the functional reputation value. A request made by the node with a negative reputation value is ignored and that node works only as a service provider and not as a requester. But if the mobile node's reputation value is more than the threshold then it can acts as a service provider and a service requester. However, functional reputation is the combination of indirect and subjective reputation values. Similarly, Buchegger and Boudec [9] proposed a novel reputation scheme known as COoperation Of Nodes, Fairness In Dynamic Ad hoc NeTwork (CONFIDANT). In this scheme, co-operation among the nodes is established based on the estimated reputation or trust value. This scheme is implemented using the routing protocol with four components, viz., monitoring component, trust component, reputation component and path manager. Among these components, the monitoring module collects the data required for estimating the reputation factor by direct interaction with mobile nodes. The reputation module estimates the trust value of a mobile node and is responsible for changing the trust value of the mobile node based on its present behaviour. Decision on isolating a malicious node from the routing path is taken by the path manager. This path manager maintains a table containing two entries, viz., (i) mobile node's unique identity and (ii) mobile node's trust value. A mobile node makes a decision whether or not to forward packets to its next-hop neighbors by checking their identities in the blacklist. Figure 3 illustrates the architecture of the trust manager component used in this approach.

Further, Rafaei et al. [10] contributed a reputation-based isolation mechanism for detecting malicious nodes by manipulating trust values of the participating mobile nodes. This mechanism implements a reputation evaluation scheme that maintains a reputation table in each mobile node with reputation index as an entry. This reputation index value indicates the reliability of a mobile node towards its participation in the routing activity. The reputation index value is incremented for every successful delivery of data packets and it gets decremented for every failure delivery of data packets to the destination. Likewise, Anantvalee and Wu [11] contributed a reputation-based system for enhancing co-operation among the mobile nodes present in the ad hoc scenario. This reputation-based system mitigates the selfish behaviour of mobile nodes either by isolating them or by encouraging

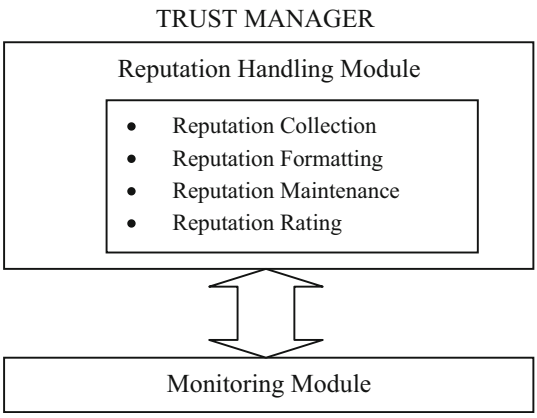

Fig. 3 Trust manager architecture

them to behave in a co-operative manner. This mechanism incorporates second hand information for manipulating reputation values. Once the reputation values are computed, these values are compared with two different threshold values in order to classify them into three different classes of mobile nodes. If the reputation value of a mobile node is above the first threshold value then the corresponding mobile node is designated as cooperative mobile node. Secondly, if the reputation value is less than the second threshold value then the mobile is identified as selfish mobile node. Thirdly, the mobile node is designated as suspicious when its reputation value lies between the first and the second threshold values, i.e., below first threshold and above second threshold value. The mobile nodes that are identified as suspicious nodes are further investigated. If they tend to become selfish, necessary actions are taken to motivate them to become co-operative and hence this mechanism is also known as co-operation encouraging mechanism. Furthermore, Wang et al. [12] presented a Co-operative On-Demand Secure Routing (COSR) mechanism to detect and isolate selfish and misbehaving nodes from the routing path of an ad hoc network. This mechanism addresses some of the issues related to DoS attacks like black-hole attack, rushing attack, worm-hole attack and selfish behaviour of mobile nodes. This mechanism detects the malicious behaviour by estimating both the mobile nodes' reputation value as well as the routes' reputation factor. These reputation factors are estimated by manipulating a mobile node's capability of forwarding which is obtained from physical layer, medium access control layer and network layer of that mobile node. Similar to CONFIDANT mechanism, COSR mechanism is implemented by incorporating four different components, viz., monitoring component, statistical analysis component, reputation component and routing component. A Secure and Objective Reputation-based Incentive (SORI) scheme was proposed by He et al. [13] in which the notion of packet forwarding ratio of a mobile node is utilized for estimating reputation. SORI utilizes three modules viz., (i) neighbours monitoring module to gather the information related to packet forwarding process of the neighbouring node, (ii) reputation propagation module to share the data with its neighbour and (iii) punishment module to discard packets. In this technique, reputation of mobile nodes is computed using the objective measures and propagated in a computationally efficient way using a one-way hash chain. Packet Conservation Monitoring Algorithm (PCMA) propounded by Tarag and Robert [14] incorporates dual information obtained from the misbehaving nodes for detecting and isolating them from routing. This monitoring algorithm targets on enhancing the reliable transmission of data

that increases the overall performance of the network in terms of PDR, throughput, total overhead and control overhead by mitigating selfish nodes. The PCMA algorithm does not rely on the information obtained from the suspicious node. This mechanism assumes that all the mobile nodes in the topology move in a collision free environment and they are capable to classify packets that are dropped due to error and congestion.

Likewise, Binglai Niu et al. [15] proposed a tit-for-tat strategy to punish the misbehaviour of mobile nodes for enforcing co-operation 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 that contains malicious nodes. This mitigation mechanism effectively deals with energy consumption and network connectivity. It also integrates two algorithms, viz., Max-improvement algorithm and Min-improvement algorithm. Recently, a Record and Trust-Based Detection (RTBD) mechanism was contributed by Senthil Kumaran and Karthikeyan [16]. This RTBD scheme analyses the detection of selfish nodes using network functions like routing and packet dropping. This mechanism accelerates the detection of misbehaving nodes and highly reduces the detection time and total overhead. This co-operative mechanism analyzes the effect of fading and interference that could originate due to the presence of selfish or malicious nodes. This mechanism identifies an optimal routing path based on a context-aware entity that detects malicious behaviour of nodes which might result in non-repudiation responses. Table 1 highlights the summary of existing history-based reputation mechanisms.

3.2 Conditional Probability-Based Reputation Mechanisms

In conditional probability-based reputation mechanism, the selfish behaviour of mobile nodes is always identified from the past and present behaviour based on their packet forwarding strategy. This conditional probabilistic mechanism quantifies the reputation of mobile nodes by measuring the current probability of genuineness based on the assumption, assertion or evidence that guarantees that the mobile node was reliable in the past. Some of the conditional probability based detection mechanisms are detailed below: In 2004, Buchegger and Boudec [17] proposed a Bayesian framework that updates and integrates reputation of mobile nodes for isolating selfishness. This isolation mechanism considers only the recent reputation rating and it is highly flexible in eliminating false information shared between the mobile nodes. This mechanism exchanges the first hand and second hand reputation information but utilizes this information only when they are compatible with the current reputation value. This method also utilizes re-evaluation and reputation fading techniques to prevent sudden exploitation of reputation. Later, in 2006, Wang et al. [18] also proposed a Bayesian network based reputation model that computes trust based on different dimensions of mobile nodes' behaviour. In this reputation model, application specific trust values are estimated and combined to determine the overall reputation of mobile nodes. Each mobile node evaluates its one-hop distant neighbors based on its own criteria which depend on the role attributed by them towards network connectivity. This reputation model also provides accurate inferences against unfair ratters. Similarly, Kargl et al. [19] contributed a trust-based evidence framework with the help of routing protocol named as SDSR. SDSR performs optimal routing decision based on the method of negotiation. In this mechanism, a node which is initially identified as selfish may get transited into a co-operative node based on dynamic change in packet forwarding process. This evidence-based framework also possesses the capacity of over-hearing and isolates selfish nodes based on the principle of exclusion. This mechanism also facilitates the detection by utilizing three monitoring techniques, viz., (i) activity-based overhearing,

Table 1 Summary of history-based reputation mechanisms with detection entity and reputation information

Authors	Detection entity	Reputation information	Highlighting features	Type of information used
Marti et al. [7]	Watch dog-based trust model	Utilizes subjective and neutral rating calculated based on watchdog and path rater	Mobile nodes need to be in promiscuous mode for monitoring	First and second hand reputation
Michiardi and Molva [8]	Watch dog-based monitoring system	Utilizes subjective, indirect and functional reputation for detection	A mobile node with negative rating can only serve as service provider	First and second hand reputation
Buchegger and Boudec [9]	Path rater-based mitigation mechanism	Maintains a blacklists that aid the mobile node in forwarding packets	Mobile nodes forward packets for their neighbours only when they are not in the blacklist of path manager	First hand reputation
Rafaei et al. [10]	Reputation index-based mitigation mechanism	Estimates the reputation index by increasing or decreasing the trust value based failure rate of packet	The failure or success of packet delivery is only estimated through TCP acknowledgement	First and second hand reputation
Anantvalee and Wu [11]	Reputation-based cooperation encouraging mechanism	Uses three levels of reputation threshold for classifying the impact of selfish node	Computation overhead of this detection mechanism is high since it requires two level of testing for identifying selfish nodes	Second hand reputation
Wang et al. [12]	Co-operative on-demand secure routing mechanism	Uses the reputation factor of mobile nodes as well as routing paths for detection	This cooperative mechanism relies only the capability of overhearing	First and second hand reputation
He et al. [13]	Secure and objective Reputation-based detection model	Uses a one-way hash chain technique for computing reputation in a computationally efficiently way	This objective model does not offer a second chance for a node to rehabilitate into selfish	Second hand reputation
Tarag and Robert [14]	Conservation monitoring algorithm	Utilizes dual information obtained from misbehaving nodes for detection	This model is weak in handling adversaries under collision dependent environment	First and second hand reputation
Binglai Niu et al. [15]	Tit-for-tat mitigation technique	Efficiently handles energy consumption and network connectivity based on max-improvement and min-improvement algorithms	This mitigation scheme relies on the opinion metric and hence it is not suitable for handling congestion	First and second hand reputation
Senthil Kumar and Karthikeyan. [16]	Record and trust-based detection scheme	Analyses the effect of fading and interference that originates due to the existence of selfish nodes	This detection scheme can only identify selfish nodes based on the context of packet forwarding	First and second hand reputation

(ii) iterative probing and (iii) unambiguous probing. Further, Chen and Varatharajan [20] proposed a Dempster Shafer theory based selfish node detection framework for estimating the degree of co-operation rendered by the mobile nodes using the concept of posterior probability. This evidence system is mainly designed for elucidating multi-dimensional attributes of random probability. It uses a numerical procedure for combining multiple evidences into a single value of evidence gathered by first and second hand reputation mechanism. Authors also used two limits of threshold called plausibility and belief for detecting the compromised nodes. These limits of threshold aid in differentiating co-operative nodes with misbehaving nodes. Khusru and Sahoo [21] presented a Predictive Probability-Based Selfishness Test (PPBST) for detecting selfish nodes using density function. This probabilistic model identifies the selfishness of mobile nodes with the aid of prior probability and Bayes theorem. Authors proved that, this heuristic model uses a selfishness test for providing higher degree of accuracy in detecting malicious nodes. In this heuristic model, misbehaving selfish nodes are identified based on Bayesian probabilistic value. This probabilistic model classifies the nodes of the network either as normal or selfish and establishes an affiliation between the nodes and their conditional probabilities towards selfishness.

Likewise, Goswami and Das [22] also contributed a probabilistic approach to detect selfish nodes using probability density function. Authors used t-distribution function for evaluating the selfishness by a Probability-Based Nodes' Selfishness Test (PBNST). This selfishness test identifies a node as selfish when the computed t-distribution based probabilistic value is <0.5. This technique also categorizes selfish nodes based on the role played by the mobile nodes in the act of effective forwarding process. Chen et al. [23] proposed an adaptive on-line algorithm that solely depends on local observations of messages for detecting selfish nodes. This adaptive algorithm uses a finite state machine model for monitoring locally observable protocol actions to generate statistical description of behaviour exhibited by each neighboring mobile node. This finite state model applies statistical analysis for clustering neighboring nodes based on their behavioural similarities. This adaptive model estimates the rate of false positives against two generic selfish strategies like route request dropping and route reply dropping. This algorithm evaluates the impact of adaptive adversary that attempts to operate in the selfish manner during detection. Furthermore, Hortelano et al. [24] proposed a probability density function based malicious detection technique that monitors mobile node based on watchdog and Bayesian filters. In this technique, initially each node employs a watchdog for detecting the

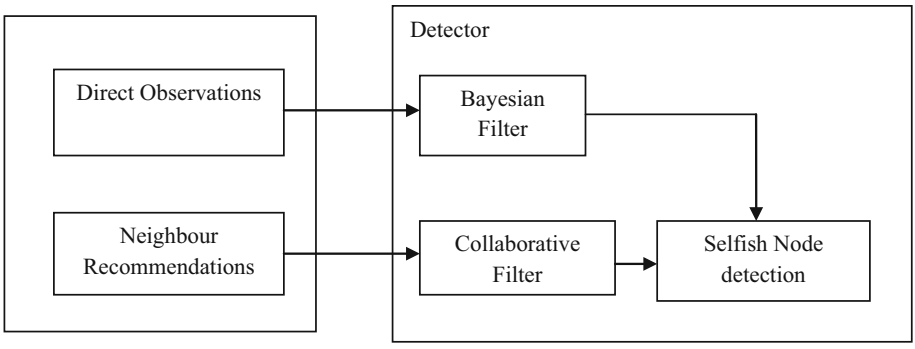

Fig. 4 Bayesian collaborative filter

misbehaviours that accounts both the number of packets forwarded and the number of packets dropped. Then the Bayesian collaborative filter shown in Fig. 4 is employed for estimating the percentage of packets that may not be forwarded in the near future. The percentage of dropped packets is compared with the threshold value and then the node is identified as malicious. This detection enables appropriate actions for preventing malicious nodes that may provide a negative impact on the network functioning and also focuses on the signaling mechanism for identifying malicious nodes.

Chun et al. [25] contributed a probability-based caching algorithm that deals with cache state interactions and common adoption policies for monitoring selfish nodes. This probability-based caching approach categorizes mobile nodes into rational, self-aware and selfish nodes based on the direct interaction with the mobile nodes present in the ad hoc environment. In addition to this, a reliability framework for identifying malicious behaviour of nodes is proposed by Zouridaki et al. [26] which is based on reputation level computed using the first and second hand information gathered from neighbour nodes. They used opinion metric as a unique factor for identifying malicious nodes.

Table 2 highlights the summary of the existing conditional probability-based reputation mechanisms for mitigating selfish and malicious behaviour exhibited by the mobile nodes present in the ad hoc environment.

3.3 Futuristic Probability-Based Reputation Approaches

In general, most of the reputation-based detection schemes proposed for isolating selfish nodes either rely on the past history of interaction between mobile nodes or on the present interaction assuming the past interaction among mobile nodes was reliable. But in some applications, the nodes' reliability needs to be forecasted by considering only the present behaviour of mobile nodes. Hence, Markov-based decision process is optimal as its memory-less property helps in forecasting the future possibility of maliciousness. This decision process estimates the future likelihood probability for quantifying reputation based on network related factors like PDR, throughput, end-to-end delay, etc. Some of the Markov-based decision models are discussed below. In 2006, Xing and Wang [27] proposed a modeling framework based on Semi-Markov process to characterize mobile nodes' behaviour in an ad hoc network. In this model, each mobile node is categorized into four different type's, viz., co-operative mobile node, failed mobile node, selfish mobile node and malicious mobile node. This model estimates behavioural probability of the mobile node by implementing a nuglet counter. This nuglet counter initially contains a token parameter with maximum value and this token value gets decremented when the node tries to forward or receive packets for its own benefits. The node possessing minimum valued token in a particular period of data transmission is said to behave in a selfish manner. The change in nodes' behaviour is predicted based on the stochastic properties and is represented using the transition probability matrix and the transition time distribution matrix. Later, in 2008, Guang et al. [28] contributed a novel mechanism known as probabilistic random back-off method for detecting selfish mobile nodes. This mechanism is specifically designed to mitigate a special category of selfish nodes that partially drops packets received from their neighbours. This mechanism is implemented by means of an enhanced Binary Exponential Back-Off (BEB) process in which each node participating in the routing activity are forced to generate a predictable random back-off interval. This probabilistic mechanism also analyses the survivability of the network with the aid of Markov chain process. In addition, authors proved that this prediction model aids in establishing maximum network connectivity even during multi-point failures that arise due to the

Table 2 Summary of conditional probabilistic reputation mechanisms with detection entity and reputation information

Authors	Detection mechanism	Reputation information	Highlighting features	Type of information used
Boudec [17]	Bayesian filter	Considers re-evaluation and reputation fading techniques to prevent sudden exploitation of trust	A priori probability is necessary for estimating detection parameters	First and second hand reputation
Wang et al. [18]	Bayesian network	Reputation is estimated only based on role played by the mobile node in forwarding process	Criteria used for quantifying reputation is dynamic	Second hand reputation
Kargl et al. [19]	Activity-based over-hearing method	Principle of exclusive and negotiation is employed for detection	The mobile node need to be in promiscuous node for monitoring	First and second hand reputation
Chen and Varatharajan [20]	Dempster Shafer theory-based evidence method	Combines multiple evidences into a numerical value	The threshold limits of belief and plausibility are not fixed	First and second hand reputation
Khusru and Sahoo [21]	Probability density function-based Bayesian approach	Uses heuristic Bayesian probability for detecting selfishness	A threshold range that predicts selfishness through conditional probability is not available	First and second hand reputation
Goswami and Das [22]	Probabilistic-based selfishness node test	Uses t-distribution parameter for detecting selfish nodes	t-distribution-based probabilistic value is not deterministic	First hand reputation
Chen et al. [23]	Finite state statistical clustering model	Estimates the rate of false positive against selfish routing strategies like dropping route request and route replies	This model depends only on local observation for analyzing behaviour of nodes	First and second hand reputation
Hortelano et al. [24]	Hybrid probability density-based Bayesian filter	Estimates the number of packets that a mobile node may forward in the near future	This mechanism consider anon-reliable signaling mechanism for selfish node detection	Second hand reputation
Chun et al. [25]	Conditional probability-based caching algorithm	Incorporates cache state interactions and common adoption policies for detection	Communication and computational overhead is high due to multilevel strategy of detection	Second hand reputation

Table 2 continued

Authors	Detection mechanism	Reputation information	Highlighting features	Type of information used
Zouridaki et al. [26]	Statistics-based conditional behavioural model	Uses a statistical prediction techniques through trust and confidence limits	The trust and confidence limits depends only on packet forwarding rate and ignores the energy consumption of mobile nodes	First and second hand reputation

presence of Further, Vallam et al. [29] proposed a non-saturated node behaviour model based on Discrete Time Markov Chain (DTMC) that addresses the issue of back-off manipulation. In this work, authors analyzed the characteristic behaviour of backoff nodes in terms of Poisson distribution. Authors also investigated the attacker detector colluding scenario by means of non-linear optimization model. This nonlinear optimization model is self analyzed by means of Sequential Probability Ratio Test (SPRT) that identifies maximum number of colluding adversaries that may arise due to inadequate energy. Similarly, Komathy and Narayanasamy [30] contributed a probabilistic node behaviour prediction model for enforcing co-operation among the mobile nodes. Authors used an energy related parameter called residual energy for estimating the impact of selfish behaviour. This model investigates the performance of the network by means of finite state Markov chain that represents the group of neighbouring mobile nodes as a single control point. This behavioural model enhances the co-operative level of mobile nodes by implementing a dynamic memory called neighbour table which periodically determines the forwarding rate of the neighbouring nodes. Authors also emphasized that the expected level of co-operation among the active mobile nodes highly depends on the ratio of packets forwarded or dropped. Xing and Wang [31] explored a Semi-Markov process-based network survivability model for enforcing reliable data dissemination. This model quantifies the impact of nodes' misbehaviour towards network survivability by analyzing its stochastic properties. This model also derives loose upper bound and tight lower bound of misbehaviour as a closed form of approximation in estimating network survivability. The upper and lower bounds of network survivability are derived by means of network size, network density, transmission range and behaviour distributions. This model also highlights that the network performance decreases with decrease in co-operation among the mobile nodes. Cardenas et al. [32] presented a malicious node detection strategy based on SPRT. This detection strategy incorporates an analytical model referred as "DOMINO" which is implemented in two steps. In the first step, the transition probability of the mobile nodes under interaction are calculated while in second step the calculated transition probability is represented using probability transition matrix and steady state probabilities are calculated for quantifying the degree of misbehaviour. In this work, authors proved that a node possesses highest probability of becoming selfish in a highly congested network environment. Likewise, Xing [33] presented a Semi-Markov process that analyses the node characteristics by means of transient and limited probability vectors elucidated malicious nodes. The authors verified that Probability Random Back-Off (PRB) enhances the fairness index on a par with BEB even in the presence of selfish nodes. These vectors aid in measuring the degree of negative impact produced by node failure and misbehaviours that affect the network reliability. This model derives a closed form of approximation and computes the

probabilistic k-connectivity parameter of the network based on node isolation analysis. It also proves that the survivability of the network rapidly decreases with increase in the probability of node misbehaviours and also verifies that DoS attacks are highly vulnerable in dense networks than sparse networks. Kadiyala et al. [34] presented an approach that incorporates Markov chain analysis for elucidating the transition probabilities that aids in determining the transmission level probabilities of all the mobile nodes present in the ad hoc network. This Markov based model provides solutions to the issues that may arise during the detection of misbehaviours and resolves the act of selfishness. This non-adaptive distributive model frames a list of conditions that need to be guaranteed for increasing the node's throughput in the presence of selfish nodes. It is highly suitable for detecting and isolating selfish nodes when the decrease in throughput of the network reaches below detection threshold. Furthermore, Hernandez-Orallo et al. [35] proposed an estimation model that measures time and cost required for isolating selfish nodes based on a watchdog mechanism. This estimation model measures the co-operation level that exists among the mobile nodes by means of Poisson distribution. This model also analyses the mobile nodes' behaviour by considering two states, viz., NOINFO and POSITIVE states. A co-operative mobile node is said to be in NOINFO state when it does not recognizes the other nodes' selfish behaviour. At the same time, it is said be in POSITIVE when it identifies its neighbour node's selfishness. This model utilizes Continuous Time Markov Chain (CTMC) based on two factors viz., (i) co-operative factor and (ii) reputation factor. Authors also inferred that the selfish nodes can be prevented by periodic diffusion.

In addition, Azni et al. [36] presented a Correlated Node Behaviour Model (CNBM) for analyzing the co-operation that exists among the cluster of mobile nodes based on semi-Markov process in continuous time. The co-operation exhibited by every mobile node is determined by analyzing various probabilistic parameters viz., probability of selfish behaviour, probability of forwarding, probability of injection, probability of loss and probability of average recovery. This model quantifies the impact of malicious nodes towards network survivability and resilience. Moreover, this model analyses the nodes' behaviour by quantifying four different parameters, viz., packet forwarding, packet dropping, packet injecting and packet loss exhibited by the mobile nodes. In this approach, the node behaviour transitions are modeled according to the correlated transition probability matrix and the transition time distribution matrix. Likewise, Azni et al. [37] also proposed an Epidemic Correlated Node Behavioral Model (ECNBM) for categorizing multi-dimensional behaviour of mobile nodes. In this node behavioural model, the selfish behaviour of mobile nodes and their dynamic transition in behaviour are estimated using Semi-Markov process. This epidemic model reduces the computational complexity by clustering mobile nodes based on its current status. This model highlights the state of mobile nodes by utilizing the concept of functional mapping that correlates the state-behaviour and the transition probabilities. Authors also proved that the extent of co-operation among active mobile nodes decrease with increase in the number of mobile nodes of the topology. In addition, they also emphasized that DoS attack decreases the network survivability and proved that the probability of network failure is significant for analyzing the connectivity for the large scale network.

Table 3 highlights the summary of the existing futuristic probability-based reputation mechanisms for mitigating selfish and malicious behaviour exhibited by the mobile nodes in the ad hoc environment.

In addition to the aforementioned selfish node detection approaches, a number of selfish node mitigation frameworks are proposed in the literature. In the following sub-section, some of the current mitigation frameworks are detailed.

Table 3 Summary of competent futuristic probability-based reputation mechanisms

Authors	Detection mechanism	Reputation information	Highlighting features	Type of information used
Xing and Wang [27]	Semi-Markov process-based node correlation model	Estimates behavioural probabilities based on nuglet counter	This node behavioural model depends mainly on the transition probability that induces a mobile node to get transferred from cooperative mode to selfish mode	Second hand reputation
Guang et al. [28]	Probabilistic random back-off method	Implements a exponential back-off process that enforces a node to generate an interval for misbehaviour monitoring	This mechanism is not capable of handling failures	First and second hand reputation
Vallam et al. [29]	Non-saturated node behaviour model-based on Discrete time Markov chain	Utilizes sequential probability ratio test for identifying colluding adversaries that arises due to inadequate energy	This model ignores selfishness that may arise due to selective dropping of packets	Second hand reputation
Komathy and Narayanaswamy [30]	Probabilistic node behaviour prediction model	Investigates the performance of the network through finite state Markov chain that considers correlated nodes as a single control point	This prediction model highly depends only on a dynamic memory of nodes called neighbour table	First and second hand reputation
Xing and Wang [31]	Semi-Markov process-based network survivability model	Quantifies the impact of node misbehaviour by analyzing the stochastic properties of mobile nodes	The closed form of network survivability called upper and lower bound of connectivity is not rigid	First and second hand reputation
Cardenas et al. [32]	Enhanced sequential probability ratio test with DOMINO	Quantifies the influence of nodes' selfishness based on steady state probabilities failure	This scheme is weak in handling selfish nodes of a dense network	Second hand reputation
Xing [33]	Transient and limited probability vector-based semi-Markov process	Measures the degree of negative impact produced by node	The probabilistic k-connectivity parameter is not rigid	First and second hand reputation

Table 3 continued

Authors	Detection mechanism	Reputation information	Highlighting features	Type of information used
Kadiyala et al. [34]	Transmission level probability-based Markov chain analysis	Provides solutions to certain issues that arise during the detection of misbehaviour and resolves the act of selfishness	This Markov chain process ignores the detection of selfish nodes that selectively drops packets	First and second hand reputation
Hernandez Orallo et al. [35]	Continuous time Markov chain analysis	Prevents the selfish nodes using periodic diffusion	This Markov chain model cannot examine the miss-detection ratio under detection delay	First and second hand reputation
Azni et al. [36]	Correlated node behaviour model	Analyses the co-operation that exists among the correlated clusters of mobile nodes	Computational complexity for clustering node behaviour is high	First and second hand reputation
Azni et al. [37]	Epidemic correlated node behavioural model	Reduces the computational complexity by clustering mobile nodes based on their current status	Functional mapping technique used in this behavioural model does effectively mitigate selfish nodes that arise due to inadequate energy	First and second hand reputation

3.4 Mitigation Frameworks for Selfish Nodes

Initially, Dhanalakmi and Rajaraman [38] presented a Reliable and Secure Framework (RSF) for detecting and isolating malicious nodes in MANET. This security framework incorporates a reliable routing algorithm for identifying a set of node-disjoint reliable paths. This algorithm constructs node-disjoint paths by estimating the number of hops and network connectivity information from every routing path. The identified disjoint reliable paths are arranged in descending order according to their reliability index. The reliability index of the path is estimated based on the number of packets received by the destination node. The estimated reliability index is sent to the source node by means of acknowledgement packets. The source node initiates transmission immediately after the identification of node-disjoint paths and further transmission takes place in the identified node-disjoint paths. The destination node initially receives the information sent by the primary reliable node-disjoint paths and compares it with the information received from all the other paths. The mismatch in the received information from the node-disjoint path indicates the presence of malicious activities in the path. Meanwhile, the destination node sends the negative feedback to the source node. Further, the source node discards the affected path from the node-disjoint multipath set for further data communication. Similarly, Konorski and Orlikowski [39] presented a novel framework that provides solution for mitigating selfish nodes using reputation methodology that incorporates Dempster-Shafer theory. The theory supports in end-to-end acknowledgement process for reliable dissemination of data. In this process, the source sends data to its destination node and waits for a

predetermined period of time for acknowledgement. If it fails to receive the acknowledgement in the stipulated period of time, it is understood that the routing path consists of maliciously behaving nodes. Then the source node sends special recommendation message to all the mobile nodes in the routing path to inform about the detected situation in the routing environment.

Furthermore, Geetha and Ramani [40] presented a trust-based multipath routing algorithm that incorporates Bayesian statistical method for secure and reliable data dissemination. This trust model establishes a set of cycle-free routing paths by considering three parameters, viz., (i) number of hops present in the route, (ii) route trust value and (iii) node trust value. The trust value of a node is estimated based on its packet forwarding rate in the past transactions which is recorded in the routing table of each mobile node. Based on the trust value, a mobile node is either rewarded or punished. The number of credits earned by the mobile node increases its participation in the routing activity. Wang et al. [41] presented a Logit regression-based trust model for service oriented MANET. This trust model dynamically estimates the trust value of source node for designating it as a service provider in MANET. The derived trust value of service provider lies in the behavioural response of mobile nodes. The derived trust value defines the probability that enables satisfactory service for the service requester in an ad hoc environment. Moreover, Soto et al. [42] in 2013 presented a multidimensional framework that incorporates physical layer features for detecting malicious and non-active mobile nodes. This framework incorporates multiple criteria analysis and nonparametric Bayesian inference method to identify the spectrum holes through which the misbehaving and failed mobile nodes are identified. This co-operative spectrum sensing framework is a distributed approach which is resilient against any type of attacks and failures. This framework is adaptable to dynamic change in behaviours that could arise in a real-time environment.

In addition, two selfish mitigation frameworks that identify selfish nodes based on multiple parameters were proposed. The first mitigation framework namely Multi-parameter Trust Framework (MTFM) was proposed by Guo and Zhou [43] for detecting and isolating misbehaving nodes. This framework incorporates multiple parameters to estimate the reputation value of a mobile node participating in the routing activity. The reputation value of a mobile node is manipulated using exponential moving average method based on grey theory by analyzing its past behaviour. This framework also aids in estimating the threshold value for detecting a malicious node in the ad hoc environment. Guo and Zhou [44] contributed a multi-vector approach called Bayesian-TRUST (B-TRUST) framework which incorporates Grey relational clustering for elucidating various types of observations which derive multiple factors that are normalized and operationally combined into a single trust vector for a mobile node. The comparative analysis of trust vector values of the mobile nodes is performed by grey relational analysis. It also effectively analyzes different types of values in the vector. The grey relational analysis derives a pre-evaluation parameter for a mobile node which is referred as Grey Relational Coefficient (GRC). Further, the trust value is estimated using grey relational analysis which utilizes GRC values.

From the survey conducted on the selfish node mitigation approaches and its frameworks, it is evident that none of the mitigation frameworks derive multiple parameters based on three context of monitoring like past history, condition probability and futuristic probability. Likewise, it is also evident that the statistical reliability coefficient is highly efficient in discriminating selfish nodes from co-operative nodes. Hence, in the next subsection, the types and roles of statistical reliability coefficient are portrayed along with their importance.

4 Need for Statistical Reliability Coefficient in Quantifying Reputation

Generally, the Reliability and Generalizability theory of statistics portrays that inconsistency in the behaviour of a mobile node can be accurately judged by reliability coefficient [45]. Further, reliability coefficients are best suited for modeling node behaviours and acts as the consistency measurement index that categorizes node behavioural values ranging from 0 to 1. In other words, the reliability coefficient represents the proportion of variation identified between the observed and expected scores of estimated behaviours. Generally, variations between scores are considered to be highly favourable as they form an unbiased estimator. Moreover, an insignificant difference of reliability does not represent a poor statistical scale of comparison as they are classified on a scale with a true zero point. Generalizability theory enhances the possibility of assessing various dimensions of mobile node's behavioural measurements. It also emphasizes that the sources used for measuring behaviour may disentangle their required inferences. In this theory, a behavioural measurement is considered as a sample from the universe of observations that could be elucidated for decision making. Moreover, the behavioural measurements of the mobile nodes are mainly used for estimating the reliability of different scores and for quantifying observable correlations. Hence, the role of the reliability coefficient needs to be investigated for understanding its applicability and suitability so that it can be used in a reliable way. Inter-rater reliability coefficient aids in testing a node's trust based on a single set of observations elucidated from its neighbouring nodes. But when multiple neighbouring nodes are used to assess a node's activity, it leads to the derivation of accurate recommendations. Hence, inter-rater reliability can be used for estimating the degree of correlation that exists between the monitored neighboring nodes in judging a monitored node. Test–retest reliability coefficient on the other hand, evaluates the reliability of a mobile node over a period of time. For instance, the reliability of a mobile node may vary with time based on its packet forwarding act, residual energy and the role played in data dissemination. Hence, a test–retest is essential for testing a node at regular intervals of time. Parallel-form reliability coefficient helps in evaluating a node's activity with multidimensional views for assessing a single behaviour.

5 Challenging Issues in the Current Approaches

Traditionally, reputation-based selfish node mitigation approaches detect misbehaving nodes based either on past history or present behaviour. From the survey conducted on the existing mitigation mechanisms, a hybrid reputation mechanism that integrates both first and second hand reputation information based on weights is not available in the literature. Majority of the hybrid history-aware reputation mechanism estimates mobile node's behaviour using statistical reliability coefficient that represents correlation or normalization by utilizing the past history. But a hybrid history-aware reputation mechanism that integrates either reliability coefficient of correlation with exponential distribution or reliability coefficient of normalization with exponential distribution is not much explored. The conditional probabilistic mechanisms available in the literature are very basic models that have been implemented either based on Bayes theorem or naive probability. The advanced techniques like Erlang distribution and Laplace Stleltjes transform-based conditional probabilistic approaches that combine two independent events influencing node's behaviour for detecting selfish nodes are not available in the literature. In addition, these

advanced conditional probabilistic mechanisms are mainly necessary for monitoring both discrete and continuous events that involve an exponential period of time for modeling node's behaviour. Further, the memory-less property of Markov process makes it highly suitable for forecasting mobile node's behaviour and the transition time between the states of mobile node's behaviour can be modeled using probabilistic distribution. But the transition time of a Semi-Markov process depends only on exponential distribution. Hence a Semi-Markov based future behaviour forecasting mechanism (forecasting the future based on present behaviour) that incorporates non birth death process is required. In addition, the selfish nodes apart from detection, they need to be classified based on the impact produced by them towards network connectivity.

6 Conclusion and Future Research Directions

The fundamental classification of selfish node mitigation approaches with the role and representations of reputation has been presented. From the thorough review on the existing literature proposed for selfish node mitigation and with the knowledge of statistical reliability coefficient, it becomes significant and essential for designing a multi-reliability factor-based selfish node mitigation framework. The framework should efficiently detect selfish nodes based on the reputation estimated using multiple parameters elucidated from three contexts of monitoring and which also categorizes and isolates selfish nodes based on the degree of influence produced by them towards network connectivity using grey relation theory. Hence, a selfish node mitigation framework that categorizes selfish nodes based on the three contexts of monitoring is necessary. But the existing frameworks proposed in the literature exclusively rely on a single type of parameter to obtain their trust values. Therefore, mitigation frameworks that detect and classify selfish nodes using multiple types of parameters need to be explored. Further, the selfish node mitigation algorithms and integrated framework preset in the literature can be extended in the following aspects.viz., (i) Existing conditional probabilistic selfish node mitigation mechanisms can be also revisited with other conditional probability estimating coefficients that calculate reputation based on Hyper-Erlang and Hypo-exponential distributions, (ii) The developed mitigation approaches can be analyzed based on mobile node survivability estimator called instantaneous availability for quantifying the degree of co-operation of mobile nodes during routing activity and (iii) The futuristic trust coefficient-aware Semi-Markov based selfish node prediction process existing in the literature can also be re-investigated by using a pure birth–death process for analyzing the possible behaviour of mobile nodes and special non-birth death Semi-Markov decision process like Markov modulated Poisson scheme.

References

1. Yau. P. W., & Mitchell. C. (2003). Reputation methods for routing security for mobile ad hoc networks. In *Proceedings of joint 1st workshop on mobile future and symposium on trends in communications* (Vol. 3, No. 5, pp. 130–137).
2. Liu. J.,& Issarny. V. (2004). Enhanced reputation mechanism for mobile ad hoc networks. In *Proceedings of trust management* (Vol. 2995, No. 2, pp. 48–62). ser. Lecture Notes in Computer Science. Springer; Berlin Heidelberg.

3. Safaei, Z., Sabaei, M., & Torgheh, F. (2009). An efficient reputation-based mechanism to enforce cooperation in MANETs. In *Proceedings of international conference on application of information and communication technologies* (Vol. 5, No. 3, pp. 1–6).
4. Chen, Y., Zhang, Y., & Yang, G. (2011). Parameter-estimation based trust model for unstructured peer-to-peer networks. *IET Communications, 5*(7), 922–928.
5. Srinivasan, A., Teitelbaum, J., & Wu, J. (2006). DRBTS: Distributed reputation-based beacon trust system. In *Proceedings of 2nd IEEE international symposium on dependable, autonomic and secure computing* (Vol. 5, No. 2, pp. 277–283).
6. Yang, L., Kizza, J., Cemerlic, A., & Liu, F. (2007). Fine-grained reputation-based routing in wireless ad hoc networks. In *Proceedings of intelligence and security informatics* (Vol. 3, No. 2, pp. 75–78).
7. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2006). Mitigating routing misbehaviour in mobile ad hoc networks. In *Proceedings of international conference on mobile computing and networking* (Vol. 3, No. 1, pp 255–265).
8. Michiardi, P., & Molva, R. (2001). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC1 16th joint working conference on communications and multimedia security: Advanced communications and multimedia security* (Vol. 1, No. 1, pp. 107–121).
9. Buchegger, S., & Le Boudec, J. -Y. (2002). Performance analysis of the confidant protocol: Cooperation of nodes fairness in dynamic ad-hoc networks. In *Proceedings of 3rd IEEE/ACM symposium on mobile ad hoc networking and computing* (Vol. 3, No. 1, pp. 226–236).
10. Refaei, M. T., Srivastava, V., & Eltoweissy, M. (2005). A reputation-based mechanism for isolating selfish nodes. In *Proceedings of 2nd annual international conference on mobile and ubiquitous systems: Networking and services ad hoc networks* (Vol. 2, No. 3, pp. 3–11).
11. Anantvalee, T., & Wu, J. (2007). Reputation-based system for encouraging the cooperation of nodes in mobile ad-hoc networks. In *Proceedings of international conference of communications* (Vol. 2, No. 3, pp. 3383–3388).
12. Wang, Y., Giruka, V. C., & Singhal, M. (2008). Truthful multipath routing for ad hoc networks with selfish nodes. *Journal of Parallel and Distributed Computing, 68*(6), 778–789.
13. He, Q., Wu, D., & Khosla, P. (2004). SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. In *Proceedings of IEEE wireless communications and neworking conference* (Vol. 1, No. 1, pp. 825–830).
14. Tarag, F., & Robert, A. (2006). A node misbehaviour detection mechanism for mobile ad hoc networks. In *Proceedings of 7th annual post graduate symposium on the convergence of telecommunications, networking and broadcasting* (Vol. 1, No. 1, pp. 78–84).
15. Binglai Niu, M. I., Vicky Zhao, H., & Hai Jiang, I. (2011). A cooperation stimulation strategy in wireless multicast networks. *IEEE Transactions on Signal Processing, 59*(5), 50–65.
16. Senthilkumar, W. J., & Karthikeyan, A. (2014). distributed framework for detecting selfish nodes in MANET using record- and trust-based detection (RTBD) technique. *EURASIP Journal on Wireless Communications and Networking, 4*(3), 31–39.
17. Buchegger, S & Le Boudec, J. -Y. (2003). Coping with false accusations in misbehaviour reputation systems for mobile ad-hoc networks. In *Proceedings of IEEE Info COMM* (Vol. 3, No. 5, pp. 49–57).
18. Wang, B., Soltani, S., Shapiro, J. K., & Tan, P.T. (2005). Local detection of selfish routing behaviour in ad hoc networks. In *Proceedings of international symposium on parallel architectures, algorithms and networks* (Vol. 2, No. 3, pp. 23–34).
19. Kargl, F., Klenk, A., Schlott, S., & Weber, M. (2004). Advanced detection of selfish or malicious nodes in ad hoc networks. In *Proceedings of 1st European workshop on security in ad-hoc and sensor network* (Vol. 1, No. 1, pp. 255–63).
20. Chen, T., & Varatharajan, V. (2009). Dempster-Shafer theory for intrusion detection in ad hoc networks. *IEEE Transactions on Internet Computing, 3*(1), 234–241.
21. Khusru, M. A., & Sahoo, G. (2013). Classication of selfish and regular nodes based on reputation values in MANET using adaptive decision boundary. *Science Research Journal of Communication Networks, 5*(1), 185–191.
22. Goswami, S., & Das, S. (2014). A probabilistic approaches to detect selfish node in MANET. *International Journal of Computer Applications, 3*(1), 23–26.
23. Chen, B., Lin Mao, J., Guo, N., Qiao, G. H., & Dai, N. (2013). An incentive detection mechanism for cooperation of nodes selfish behavior in wireless sensor networks. In *Proceedings of 25th control and decision conference* (Vol. 6, No. 3, pp. 4021–4024).
24. Hortelano, C., Calafate, T., Cano, J. C., de Leoni, M., Manzoni, P., & Mecella, M. (2010). Black-hole attacks in p2p mobile networks discovered through Bayesian filters. In *Proceedings of OTM workshops* (Vol. 2, No. 6, pp. 543–552).

25. Chun, B. -G., Chaudhuri, K., Wee, H., Barreno, M., Papadimitriou, C. H., & Kubiatowicz, J. (2004). Selfish caching in distributed systems: A game-theoretic analysis. In *Proceedings of the 23th Annual ACM symposium on principles of distributed computing* (Vol. 7, No. 4, pp. 21–30).
26. Zouridaki, C., Mark., B. L., Hejmo, M., & Thomas, R. K. (2005). A quantitative trust establishment framework for reliable data packet delivery in MANETs. In *Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks* (Vol. 1, No. 4, pp. 1–10).
27. Xing, F., & Wang, W. (2006). Modelling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes. In *Proceedings of IEEE conference on communication* (Vol. 2. No. 5, pp. 1879–1884).
28. Guang, L., Assi, C., & Benslimane, A. (2008). Enhancing IEEE 802.11 random back-off in selfish environments. *IEEE Transactions on Vehicular Technology, 57*(3), 1806–1822.
29. Vallam, A., Franklin, & Murthy, C. (2008). Modelling co-operative MAC layer misbehaviour in IEEE 802.11 ad hoc networks with heterogeneous loads. In *Proceedings of 6th international symposium on modelling and optimization in mobile Ad Hoc and wireless networks* (Vol. 5, No. 3, pp. 197–206).
30. Komathy, P., & Narayanasamy, K. (2007). A probabilistic behaviour model for selfish neighbour network wireless ad hoc network. *International Advances in Surgical Oncology Journal of Computer Science and Network Security, 7*(7), 77–82.
31. Xing, F., & Wang, W. (2010). On the survivability of wireless ad hoc networks with node misbehaviours and failures. *IEEE Transactions on Dependable and Secure Computing, 7*(3), 284–299.
32. Cardenas, A., Radosavac, S., & Baras, J. (2007). Performance comparison of detection schemes for Mac layer misbehaviour, In *Proceedings of 26th IEEE international conference on computer communications* (Vol. 4, No. 5, pp. 1496–1504).
33. Xing, F. (2009). Modelling, design, and analysis on the resilience of large scale wireless multi-hop networks, Ph.D. Dissertation.
34. Kadiyala, M., Shikha, D., Pendse, R. & Jaggi, N. (2011). Semi-markov process based model for performance analysis of wireless LANs. In Proceedings of international conference on pervasive computing and communications workshops (Vol. 5, No 7, pp. 613–618).
35. Hernandez-Orallo, E., Serrat, M., Cano, J.-C., Calafate, C., & Manzoni, P. (2012). Improving selfish node detection in MANETs using a collaborative watch-dog. *IEEE Communications Letters, 16*(5), 642–645.
36. Azni, A., Ahmed, R., Noh, Z. A. M., Basari, S. H., & Hussin, B. (2013). Correlated node behaviour model based on semi markov process for MANETs. *International Journal of Computer Science, 9*(9), 25–32.
37. Azni, A., Ahmed, R., Muhamed Noh, Z., Basari, S. H., & Hussin, B. (2013). Epidermic modelling for correlated node behavior in ad hoc network. *International Journal of Chaotic Computing, 1*(1), 67–76.
38. Dhanalakshmi, S., & Rajaram, M. (2008). A reliable and secure framework for detection and isolation of malicious nodes in MANET. *International Journal of Computer Science and Network Security, 8*(10), 184–190.
39. Konorski, J., & Orlikowski, R. (2009). A framework for detection of selfishness in multihop mobile ad hoc networks. *Journal of Telecommunications and Information and Technology, 2*(2), 34–40.
40. Geetha, S., & Ramani, G. (2012). Trust based secure multipath OLSR routing protocol in MANET using fuzzy theory. In *Proceedings of 2nd international conference on computational science, engineering and information technology* (Vol 6, No. 3, pp. 120–125).
41. Wang, Y., Lu, Y. C., Chen, I., Cho, J. C., Swami, A., & Lu, C. (2014). Logittrust: A logit regression-based trust model for mobile ad hoc networks. In *Proceedings of 6th ASE international conference on privacy, security, risk and trust* (Vol. 5, No. 3, pp. 12–22).
42. Soto, D., Quezada, L., & Cordova, F. M. (2013). Evaluation of the perspectives of balanced scorecard through of a multicriteria analysis analytic network process (ANP). *International Journal of Industrial and Systems Engineering, 13*(3), 298–308.
43. Guo, J., & Zhou, B. (2014). A multi-parameter prediction model for misbehaviour detection in a MANET trust framework. *Journal of Applied Science and Engineering, 17*(1), 45–58.
44. Guo, J., & Zhou, B. (2011). A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks. In *Proceedings of IEEE Tust Com-11* (Vol. 4, No 2, pp. 142–149).
45. Webb, N. M., Richard, J., Shavelson., & Haertel, E. H. (2006). Reliability coefficients and generalizability theory. In *Handbook of statistics* (Vol. 26, No 1). Elsevier press.

J. Sengathir born in 21st December 1982, has received his B.Tech. in Computer Science and Engineering and M.Tech. in Information security from Pondicherry Engineering College, Pondicherry, India. Currently, he is pursuing his Ph.D. in Computer Science and Engineering from Pondicherry Engineering College, Pondicherry, India. His fields of interest include Mobile Ad hoc Networks and Software Engineering.

R. Manoharan is currently working as a Professor in the Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India. He has more than twenty years of experience in teaching and research. He has published many reputed International Journals and Conference papers highlighting the area of Internet Technology, Software Engineering, High speed networks, Mobile Ad hoc Networks and Vehicular ad hoc networks.