Cooperation Stimulation Mechanisms for Wireless Multihop Networks: A Survey

Normalia Samian[a,*], Zuriati Ahmad Zukarnain[a], Winston K. G. Seah[b], Azizol Abdullah[a], Zurina Mohd Hanapi[a]

[a] *Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400, UPM Serdang, Selangor, Malaysia*
[b] *School of Engineering and Computer Science, Victoria University of Wellington, Wellington 6012, New Zealand*

Abstract

In wireless multihop networks such as wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs), nodes have to rely on their peer neighbours in transmitting packets to intended destinations. A successful rate of communication in these networks is assured if all nodes in the network fully cooperate to relay packets for each other. However, due to the existence of nodes with various motives, cooperativeness cannot be ensured and the communication goal is not achieved. Consequently, many cooperation stimulation approaches have been proposed to address node selfishness by using, broadly, incentive-based and punishment-based approaches. These schemes consist of several components including monitoring mechanisms, that need to be optimized in order to provide effective ways to detect and manage selfish nodes in the networks. This article summarizes existing cooperation stimulation mechanisms and discusses important issues in this field such as false judgment and node collusion, whereby the root of these kinds of problems originates from the inability to obtain accurate evaluation on the behaviour of a node.

Keywords: Cooperation, Selfish behaviour, Wireless multihop networks, Incentive schemes, Punishment schemes, Game theory, Accurate behavioural evaluation, False judgment, Node collusion

1. Introduction

Wireless multihop networks consist of autonomous nodes that perform network tasks in a self-organizing manner. The networks, which is categorized as infrastructure-less includes several class of networks such as wireless sensor networks (WSNs), mobile ad hoc networks (MANETs), wireless mesh networks (WMNs) and vehicular ad hoc networks (VANETs) [1, 2]. As they are infrastructure-less, there is no central controller or wired backbone to handle the communication process. Therefore, the nodes in these networks have to act as routers and hosts simultaneously and utilize hop-by-hop packet transmission. Consequently, with these processes occuring in the network, high frequency of communication among peer nodes is expected. Examples of applications utilizing wireless multihop networks for data transmission exist in military battlefield, catastrophe recovery, event monitoring sites, vehicular ad hoc technology system, health monitoring services and many other civilian applications. As applications based on wireless multihop networks have evolved rapidly, much attention has been given to address issues that may affect the performance of such networks. These include issues related to resource constraint, security, cooperation and connectivity where the main concern is to ensure that data can be efficiently transmitted across the networks to reach intended recipient. In the case where packets that need to be transmitted are between nodes within direct wireless transmission range, a successful rate of data transmission is assured if connectivity is good. However, when the source and destination nodes are beyond direct wireless transmission range of each other, the source node has to rely on relay nodes or intermediaries to help forward the packets towards intended destination node.

*Corresponding author. Tel: +60389471777
Email addresses: normalia@upm.edu.my (Normalia Samian), zuriati@upm.edu.my (Zuriati Ahmad Zukarnain), winston.seah@ecs.vuw.ac.nz (Winston K. G. Seah), azizol@upm.edu.my (Azizol Abdullah), zurinamh@upm.edu.my (Zurina Mohd Hanapi)

When dealing with relay nodes in wireless multihop networks, the issue of uncooperative forwarding behaviour will most likely occur because each node has different motivations and intentions. The intentions are very subjective and may result in good, selfish or malicious behaviours. Ideally, if each node shows a good behaviour by cooperatively relaying packets from other nodes, an optimum network performance can be achieved. However, such assumption is not valid in the real environment of wireless multihop networks where nodes are autonomous and most importantly, have resource constraints. With these characteristics, nodes are compelled to preserve their own energy to sustain in the network, which is why cooperative relaying is difficult to achieve. This behaviour is known as selfishness and can exist in any node, affecting topology design [3] and network operations like routing and packet forwarding [4]. The level of selfishness can be very abstract, making it difficult to measure and quantify because unlike a node with malicious intent, selfishness may be shown intermittently depending on the network scenarios that it needs to handle. For example, if a node is handling heavy forwarding loads due to its location being the closest to a particular hectic destination, it may decide to favour certain requesting nodes or drop any incoming packets that arrive after certain forwarding periods to avoid excessive energy depletion. From the energy conservation principle, such behaviour is reasonable for a node's own benefits but if it is done excessively and unfairly, the final effect towards the network may be the same as those by malicious nodes.

In contrast to malicious nodes which intentionally plan to disrupt network services through harmful attacks, selfish nodes do not mean to harm the network. However, the effect of selfishness may eventually cause network disruption if all nodes decide to be self-centred by not forwarding packets for other nodes. Although selfishness can be classified as a type of malicious behaviour, it may not be effectively overcome with security approaches. Generally, security approaches are often implemented using cryptographic-based mechanism in order to thwart bad nodes from the network such as in [5, 6]. Although this kind of security mechanism may work well in reducing selfishness, it has high computational overheads and is not a suitable countermeasure for selfish nodes, which are not as malign as malicious nodes. Hence, cooperation mechanisms have been introduced to solve the problem of selfishness by detecting nodes that show uncooperative behaviour and provide a means to discourage selfishness (i.e. stimulate cooperativeness) using either incentive-based or punishment-based mechanisms.

The main contribution of this article is to present a comprehensive study on the existing cooperation stimulation mechanisms by investigating the strengths and weaknesses of their key structures and elements. Using comparative analysis, we have identified crucial issues that revolve around the selfishness detection aspect of this specialized field, which is rooted in the inability to accurately evaluate node behaviour. The remainder of this paper is organized as follows. Section 2 presents an overview of research on wireless multihop networks with a focus on cooperation. Discussion on cooperation stimulation mechanisms is presented in Section 3 where existing schemes (i.e. credit-payment, reputation, hybrid and punishment schemes) are reviewed and discussed from several important angles. This section also discusses game theory, which is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers" [7] and widely applied in the study of cooperation in wireless networks. In Section 4, a comparative analysis based on overall structure and elements of cooperation schemes is carried out and summarized in Table 3. We extracted several important features from each existing scheme, identify strengths and weaknesses for possible enhancements. We also provide discussion on game theory of perfect/imperfect public/private monitoring as an alternative to available observation tools. Section 5 discusses the open research issues of this field specifically on false judgment and node collusion problems, and highlights the main reasons behind the prevailing problems. This section also provides some insights on what should be anticipated for future directions of node cooperation mechanisms for wireless multihop networks. Section 6 concludes this paper.

2. State of the Art of Wireless Multihop Networks

Extensive research have been conducted to overcome the issue of cooperation in wireless multihop networks. As depicted in Figure 1, this issue can be investigated based on two broad approaches: (1) full cooperation and (2) partial or zero cooperation, as shown in Figure 1. These two categories are described further in the following subsections.

2.1. Full Cooperation

In this category, all nodes are considered to be fully cooperative in any communication operation. This has been the fundamental assumption in wireless multihop networks where research focused on the improvement of relaying

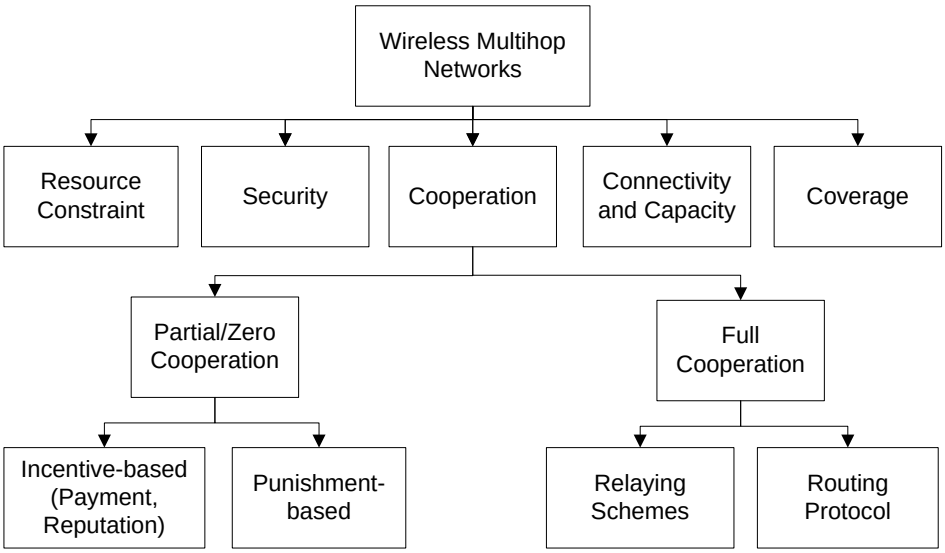


Figure 1: State of The Art of Wireless Multihop Networks.

schemes and routing protocols, as depicted in Figure 1. Research on the improvement of relaying scheme proposes cooperative relaying techniques, also known as cooperative communication (CC), and the introduction of extensions to improve performance. In the work by Herhold *et al*. [8], the performance of conventional relaying versus cooperative relaying in multihop wireless networks was analyzed and compared. Conventional relaying occurs when a node only listens or obtains information from preceding relay node and thus, the destination node only gains information from the last relay in the transmission path. Meanwhile, cooperative relaying contributes information to the destination by putting together all information from each relay node. The performance is measured based on how these two techniques (as also compared to direct transmission) impact communication reliability in term of path loss, different relay positions and spectral efficiency. Sharma *et al*. [9] proposed an improvement for CC in wireless multihop networks by looking at the issues of joint routing and relay node selection during multiple transmission sessions at one particular time. In a multihop session, when two or more traffics are initiated at the same time, tasks overlap will most likely occur. For instance, a source node that initiates a communication session can simultaneously become a relay node when another transmission session requires it to be an intermediary, causing a cross-function problem, thus reducing throughput. The authors utilized a mathematical model of branch-and-cut framework and proposed few new components (i.e. Feasible Solution Construction (FSC) algorithm, cutting plane and branching variable) within the framework in order to optimize the effectiveness of CC. The goal of implementing the framework was to minimize task redundancies to achieve optimum throughput.

In [10], the issue of relay node assignment in multiple source-destination nodes under cooperative ad hoc networks was highlighted. The specific problem occurs when more than one source-destination pairs want the same set of relay nodes to transmit data. When this occurs, the rate of data transfer is low due to non-optimized utilization of available relay nodes which become wasted resource. In order to achieve efficient relay node allocation, the authors proposed a polynomial-time algorithm named Optimal Relay Assignment (ORA). The algorithm generally works by maintaining linear complexity of the relay assignment in each loop, whereby available relay nodes are distributed evenly to the source-destination pair nodes, thus increasing data transfer rate for each pairs as proved by the simulation results of this paper.

On the other hand, the full cooperation approach has also been investigated from the perspective of routing protocol enhancement, which aims to increase the efficiency of communication operation. In [11], the authors aim to provide an efficient communication operation in multi-source multi-destination multihop wireless networks by proposing a distributed routing scheme with collision avoidance strategy. Their paper focused on collisions that occur when two or more source nodes transmit data over one intermediate node at the same time. The authors suggested that instead of allowing collisions at the intermediate node, there should be an alternative node to carry out the transmission task.

Thus, they introduced the concept of virtual node and virtual link. A virtual node consists of a collection of several nodes that cooperatively receive or send data to a receiver node, whereas a virtual link is the link that is associated with the virtual node. By having a virtual node, nodes within the group would cooperatively decide on which node is more deserving of the transmission process. Hence, collision and bottleneck could be avoided.

In [12], the authors proposed an extensive framework of cooperative protocols for wireless ad hoc networks. They focused on utilizing cooperative relaying in three layers of OSI: physical, data link and network. For physical layer, unlike most works that only considered one type of scheme, this work provided the flexibility of using repetition or space-time coding scheme. Furthermore, the coding scheme is supported by proposed MAC extensions, which are maximal ratio combining-MAC (MRC-MAC) for repetition coding and space-time coding-MAC (STC-MAC) for space-time coding in data link layer to support cooperative relaying. On the other hand, a cooperative routing protocol (CRP) has been proposed for network layer to ensure reliable transmission from source to destination node. Since AODV routing protocol was used as a platform, the authors also proposed an enhanced-CRP (E-CRP) to solve the gray zone problem in AODV, which occurs when data packets are not transmitted after a valid route has been established.

In another study [13], the goal was to produce an energy-saving communication process in wireless network (at physical and network layers) through cooperative routing mechanism. The authors proposed an optimal cooperative routing algorithm through dynamic programming (DP) concept and introduced two sub-optimal algorithms to minimize energy-usage in route establishment process. The algorithms limited the number of transmitted messages to one in a particular transmission session that help to attain optimal energy-saving by selecting the minimum-used-energy route. However, the study did not consider the effect of having more than one message being transmitted in a route and the existing of multiple flows in the network.

2.2. Partial/Zero Cooperation

Partial/zero cooperation is a condition where fully cooperative behaviour cannot be guaranteed. The scenario is especially likely for ad hoc networks where mobile devices have portable power sources with limited amounts of energy, which drives nodes to behave selfishly. Under partial or zero cooperation, the approaches that have been proposed are classified into two major categories, namely, incentive-based and punishment-based mechanisms. Both approaches have been widely implemented in wireless multihop networks, specifically to handle misbehaved node in the network layer by obtaining information on node forwarding behaviour prior to taking necessary actions.

Two main types of misbehaviours exhibited by nodes are maliciousness and selfishness. Malicious is an attribute of nodes that intentionally disrupt network operation by launching either passive or active attacks, severely paralyzing the network. However, such an action is usually visible and can be controlled by using security countermeasures. It is the latter (i.e. selfishness) that is trickier to capture because it is rarely displayed explicitly by a node. A selfish node does not have the intention to flood the network with malicious injections, but the act of abstaining to cooperate may also collapse the network. In other words, network disruption is a targeted goal of malicious nodes but it is a final outcome of selfish nodes. In order to handle selfishness, cooperation stimulation mechanisms have been introduced in many existing related works and detailed discussion is presented in Section 3.

3. Cooperation Stimulation Mechanisms in Wireless Multihop Networks

The direction of discussion for this section is based on the two major classifications of cooperation stimulation/selfishness mitigation mechanisms, viz., incentive-based and punishment-based mechanisms/schemes as shown in Figure 2. The main goal of these proposed schemes is to enforce cooperation of nodes to achieve optimal network performance that can be measured using performance metrics like throughput, packet delivery ratio, accurate behaviour detection rate, etc.

3.1. Incentive-based Mechanism

Incentive-based mechanism is an approach that has been proposed to provide motivations for nodes to cooperate in the form of credit payment or reputation award (viz. good or bad), following the observation and evaluation on the forwarding behaviour of a particular node.

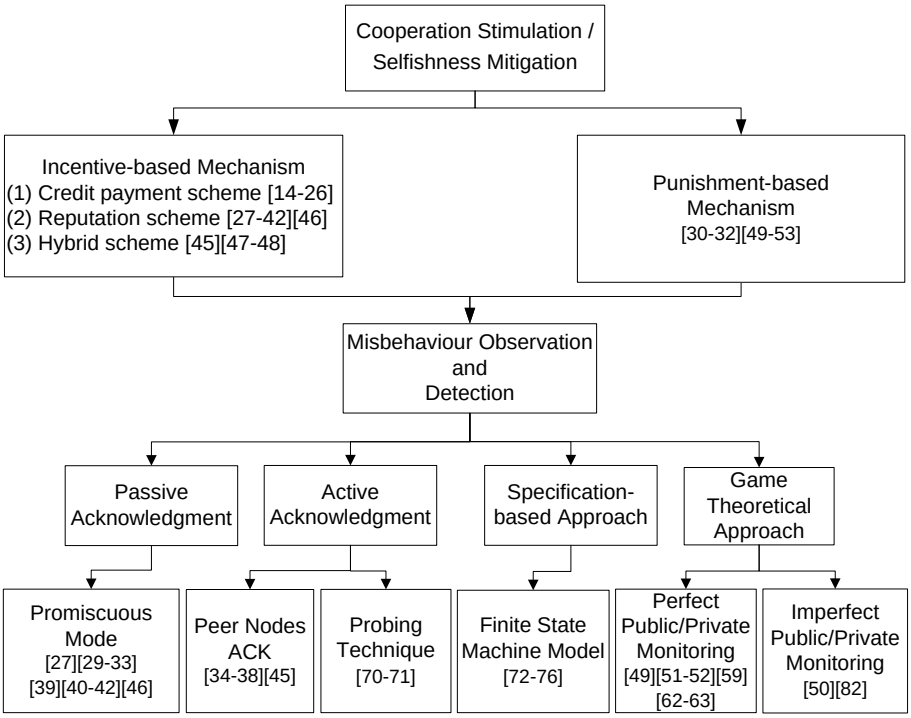


Figure 2: Classification of Cooperation Stimulation Components

3.1.1. Credit Payment Scheme

The concept of virtual credit has been introduced under the payment scheme, which a node holds as a way to represent their cooperativeness. The amount of credit will increase when a node helps to forward other nodes' packets and decrease when it refuses to cooperate. When a node runs out of credit, it will not be able to send its own packets. Thus, collecting credit by forwarding packets for others becomes the motivation for nodes to be cooperative. Method of payment for nodes can be viewed from two main aspects, viz., distributed and centralized architectures, whereby reliance on tamper-proof hardware and central-agent are involved respectively.

Distributed Architecture

In terms of the scalability aspect, a distributive payment method offers advantages for nodes to administer their own credits such that prompt transactions can be done more conveniently using the tamper-proof device installed in each node; credits are charged and paid according to node's sending and forwarding operations without having to rely on a third-party manager. Examples of credit schemes that implement tamper-proof device are [14, 15].

A virtual currency called nuglets rewards nodes that cooperatively help in forwarding packets [14]. The payment system worked based on two models known as Packet Purse Model (PPM) and Packet Trade Model (PTM). In PPM, a source node pays all its forwarders along the path to destination by appending sufficient nuglets in the packet. Each intermediate node will take some nuglets according to its forwarding cost and if there is no nuglet left, the packet is dropped. Hence, it is important for a source node to avoid under estimation of nuglets. In PTM, nuglets are not appended in a packet, instead they are traded via buying and selling activities among intermediaries in order to forward the packet where the destination node will eventually pay for the total cost. This method helps to reduce the number of dropped packets due to under estimation of nuglets by the source node, but it may cause node to lose their nuglets unnecessarily, such as, when intermediaries refuse to buy the packets (i.e. being uncooperative). The scheme was enhanced in [15] by introducing credit-counter to reduce overloading of packets by a source node. The counter will increase when a node helps in forwarding packet for others and decrease when it sends out its own packets. Thus, a node must balance its forwarding activities, so that the counter will remain sufficient in order to survive in the network.

Despite having the ability to provide flexibility for nodes to manage credits, distributed-based credit scheme does not gain wide adoption due to the following factors:

- ***Cost*** - as the name implies, the tamper-proof device is claimed to be resistant from being tampered by any forgery attacks which reflects costly hardware. It might not be practical for every node to have such a security device considering that the usage might not achieve optimum level.
- ***Resistance Level*** - although the device might be durable from external attack, it can still be manipulated by its owner to collude with other nodes and perform fraudulent transactions. In certain cases, it has to be assumed that the device could provide optimal security protection [16] but such an assumption might not hold in many real scenarios.
- ***Unfairness*** - due to nodes' dispersed locations, getting fair opportunity to obtain credits for continuous network operations is hard. Nodes which are located in the middle of the network will have more opportunities to forward packets for other nodes (gain credits), whereas, nodes on the periphery of a network have smaller chances to be selected to participate in the communication process (lose credits). When credits cannot be distributed evenly in the network, resources (i.e. potential cooperative forwarders) have the tendency to be wasted, thus, cooperation cannot be ensured.
- ***Excessive Overheads*** - a node needs to forward enough packets to gain credits for its own packets to be sent out and possibly forwarded by other nodes. In the event of major packet loss or dropped packets, the amount of credits earned by a node may not be sufficient to cover the cost of re-sending its packets. In this case, a node is charged more, with no guarantee that its packets will be forwarded optimally.

Centralized Architecture

Another method of credit payment is based on centralized architecture where reliance on central agent (i.e. bank) to manage credit transactions is involved. Credit is paid before or after a particular node is charged or rewarded, by submitting receipts/reports to the central agent for verification and issuance of payment. Receipts submission can either be done online (on-the-go transaction with the bank) or offline (accumulated transactions sent in batch to the bank). Having reliance on a central agent removes the need for each node to manage credit transactions, thus, reducing the processing burden and the need to have tamper-proof device. Nonetheless, this approach comes with several drawbacks whereby bottleneck problem during communication with the central agent is the most pronounced issue. We will first briefly discuss existing schemes based on this approach prior to presenting its pros and cons.

In Sprite [17], nodes keep a receipt of its forwarding activities and claim for payment from a central agent named Credit Clearance Service (CCS). To prevent the payment from being pushed to the destination node by the source or/and colluding nodes, only the source node is charged for packet transmissions it has initiated, and forwarders gain credits only if the CCS received satisfactory proof from corresponding next-hop nodes stating that forwarded packets have been received successfully. Anderegg and Eidenbenz [18] proposed a payment-based scheme that functions as underlying concept in their design of routing protocol named Ad hoc-VCG. VCG, which stands for Vickrey [V], Clarke [C] and Grove [G] adapted a pricing-based mechanism called the second-best sealed bid auction. Ad hoc-VCG protocol was designed with the aim of establishing a routing path that is cost-efficient and reliably truthful where every node is required to genuinely publish its cost of energy during the route discovery session. A source node will choose the most cost-efficient (energy-wise) and truthful (policy-obedient) route to send its data packet and pay the intermediate nodes via the central bank. This approach is similar to PPM model proposed in [14] except that forwarding cost of each intermediary needs to be published beforehand to eliminate the problem of over/under estimation of cost by source node. A game theoretical technique was also proposed to ensure truthfulness. Ad hoc-VCG was shown to be effective in finding energy-efficient and truthful route but with assumption that all nodes genuinely declare their real cost and there is no collusion among nodes to illegally maximize payment; this was not addressed in the work.

An enhanced version of Ad hoc-VCG, COMMIT protocol [19], allows a source node to negotiate an affordable cost with the intermediaries rather than leave the decision to the intermediaries. In the initial route discovery process, a source node or sender will announce the maximum total cost that it can offer if a connection is established. Upon

receiving packets containing such information, intermediaries will decide whether to receive or reject the offer. Assuming that all related intermediaries agree with the offered payment and that a routing path is found, the destination will return all gathered information to sender. If the requested total payment is lesser than the offered amount, sender would choose the route. Even though the sender gains control over the amount of payment, the processes that it needs to go through are quite tedious and can lead to high communication overhead. In reality, it is difficult to achieve total agreement by intermediaries on the offered amount, unless the sender can provide a flexible amount of payment. Janzadeh *et al*. proposed a scheme known as Express [20], which is a credit-based mechanism that inherits some common features of Sprite [17], except that it offers a lighter computational overhead, while providing a secure credit transaction by adopting hash chains instead of digital signatures for authentication. The efficiency of the proposed scheme was ensured by overcoming any cheats with necessary incentives and penalties. In [21], a secure credit payment scheme named Report-based pAyment sChemE (RACE) was proposed. RACE is a secure scheme that aims to have low communication and processing overhead due to the dependability on central agent. It was done by the introduction of lightweight payment reports that need to be submitted to the agent, instead of using common receipt. The term lightweight is defined as having less information appended on the reports, yet still sufficient to provide necessary information. Extra information will be submitted to the central agent only when the need arises like when a node requires more evidence on a cheating node. Furthermore, the evidence will only be stored temporarily to reduce storage overhead. The efficiency of the proposed scheme was validated by their analytical and simulation results.

The centralized architecture has been receiving wider acceptance in comparison to the decentralized approach and has been adopted in many other credit-based schemes [22, 23, 24, 25]. Although the centralized approach offers several advantages, especially by removing the reliance on tamper-proof device, it comes with several drawbacks (including the aforementioned unfair share problem suffered by the distributed architecture) like high communication and processing overheads, verification delay and false verifications, increased storage overheads, and the need to secure the central agent as well as information held by it. As both distributed and centralized architecture have pros and cons, a hybrid scheme named CASHnet [26] has been proposed by combining the good features of both architectures. In CASHnet, the use of tamper-proof device (via smart card) is preserved to provide flexibility for nodes to manage their credit transactions while at the same time depending on a centralized service station to top-up a node's credits. Although CASHnet is able to maintain credits in the network in the long-run, it still suffers from high protocol overhead.

3.1.2. Reputation Scheme

Reputation is another type of incentive used to stimulate cooperation in wireless multihop networks. A node collects the past behavioural information of other nodes based on its own observations, reports from trusted neighbours, or both. The information, indicating their level of selfishness, is used to determine the reputation value of monitored nodes. A reputation level lower than a predetermined threshold value may reflect that a particular node is selfish, thus will be avoided during the communication process. The most essential element in measuring reputation is to determine a node behaviour via techniques like passive and active acknowledgment (cf: Section 4.1). Once a node behaviour has been determined, it will be passed to the reputation system components for further evaluation.

Rating/Voting Mechanism

Rating/voting is an essential element in a reputation scheme whereby an observer node rates the level of cooperativeness/selfishness of a node in routing and forwarding packets. Subsequently, the rating may be shared in a voting system to further evaluate a node's behaviour by collecting opinions from other nodes prior to enforcing punishment towards a selfish node. Among important aspects that need to be considered under this element are how to rate a node's behaviour, how to process votes from nodes to compute the reputation level, how to share the votes effectively and how to ensure that the shared votes are not falsified.

Early work adopting the rating mechanism for reputation involved monitoring nodes' activities using a watchdog mechanism [27], in which the information gathered is used to rate a node such that a node with low rating is excluded from the routing path (pathrater). The work in [27] is considered as the pioneer in utilizing promiscuous mode of operation to obtain a node's forwarding activities, whereby a watchdog node observes (i.e. listens) the next hop neighbour in order to know whether it helps to relay received packets or simply discards them. Continuously discarding packets causes the misbehaving rate of a particular node to increase and when the rate surpasses a predefined threshold value,

it is labeled as misbehaved and is avoided in the next route establishment process as a form of punishment. However, such an action will actually benefit the misbehaved node in the sense that its forwarding burden is lessened by not committing to the communication process initiated by other nodes.

Reputation schemes that had adopted promiscuous mode as a monitoring tool and used rating/voting include CONFIDANT [28], CORE [29] and SORI [30]. CONFIDANT (Cooperation of Nodes: Fairness in Dynamic Ad Hoc NeTworks) [28] aims to develop a better path rating mechanism. Misbehaviour is detected by neighbourhood nodes where information is sent to a reputation system (i.e. voting mechanism) that collects sufficient evidences and votes from observing nodes. Collaborative Reputation (CORE) [29] was introduced to overcome the problem of node falsification in CONFIDANT by restricting dissemination of negative rating across the network, which means that the mechanism only allows nodes with good rating to be announced so that any attempt of falsification by colluding nodes remains in vain. However, false announcement could still happen when nodes collaboratively rate a bad node as good, and thus, impairing the credibility of the announcement. In both of these schemes [28, 29], the reputation information is broadcast globally causing high communication overheads. Secure and Objective Reputation-based Incentive (SORI) [30] was introduced to reduce the overhead by sharing information on the reputation of a node with its neighbouring nodes only.

On the other hand, work on mitigating the adverse effect of globally shared reputation information have been proposed by emphasizing and enhancing the ability of local observation. In [31], a scheme named Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) was introduced to fully utilize the advantage of first-hand/local observation to avoid global exchange of reputation information that is prone to manipulation by colluding nodes. Each node keeps the rating information of its neighbours in the same wireless channel area, where the default rating value is neutral. The value will either increase or decrease according to the forwarding actions taken by the neighbours. If the rating value of any neighbour falls below a certain threshold, that particular node will be added to a *faulty list* and, as punishment, any request for services from this node will be rejected; a decision made locally by an observing node. A unique feature of this scheme is the introduction of a second chance element whereby after a punished node has been inactive for a certain amount of time, it will be moved from the faulty list and given another chance to increase its rating by being cooperative. This element was found to help in reducing false judgment, where any node that was mistakenly labelled as misbehaved obtains another chance to vindicate itself.

OCEAN was proven to perform better than a generic scheme which utilizes globally shared reputation information due to the reduction of node collusion risk. However, the scheme is still unable to cope well with the reliability of a local decision made by any node, as it is possible that a node falsely accuses other nodes as misbehaved. In addition, the faulty list can also be tampered by attacker. The weaknesses in OCEAN were later addressed by a scheme called Hybrid Mechanism to Enforce Node Cooperation (HEAD) [32] which utilizes warning messages instead of relying on broadcasting faulty list during the route discovery phase. The scheme proposed in [33], known as Locally Aware Reputation System (LARS) also emphasized on the use of local/direct observation rather than globally-shared information on reputation, which can cause high communication overhead and the risk of colluding nodes. Once an observed node's reputation value falls below a predetermined threshold due to the act of dropping packets, its selfishness will be identified, and a warning message (signed with signature) of the behaviour will be signaled to k-hop neighbours.

Another approach involves the use of end-to-end and hop-by-hop acknowledgment mechanism to overcome the issue of colluding nodes giving false accusation or false praise on a node behaviour [34, 35, 36]. On the other hand, hop-by-hop acknowledgment such as [37, 38] was introduced to reduce the adverse effect of accusing whole link as unreliable imposed by end-to-end acknowledgment method.

Trust Management

In determining the threshold level of bad and good reputation, node behaviour may be assessed by its trustworthiness level which can be derived based on trust features or evidences. There have been several methods proposed to compute trust metrics to evaluate node trustworthiness and thus, determine node selfishness that will be discussed in the following existing existing schemes.

To obtain stronger evaluation of a node behaviour, CONFIDANT [28] introduced a *trust manager* that cross-checking a particular misbehaviour report prior to making announcements. However, this scheme is susceptible to false accusation by colluding nodes towards a well-behaved node. Besides, the reliability of the trust manager's opinion is questionable due to its vague functionality. Chong *et al.* proposed a detection framework named Separation

of Detection Authority (SDA) [39] to improve the trustworthiness of shared information on behaviour by delegating the task of detecting selfish nodes to three different entities, named reporters, agents and central authority. When a node (i.e. reporter) finds out about the selfish behaviour of a particular node, it submits a report to the central authority that is going to investigate the report by appointing agents (i.e. neighbours of the suspected nodes) that would also observe the node. Assuming that all agents would submit their reports to the central authority, a final evaluation is made based on majority votes by the agents. Although this approach seemed to succeed in detecting selfishness by having a central authority to validate reports, the process is costly due to the need to send and receive additional investigation packets. In addition, due to the need for second-hand observations, SORI and SDA share the same weaknesses as CONFIDANT and CORE such that a reputable node may falsely report a node as having the correct behavioural state (i.e. falsely accuse or falsely praise [40]) and having the erroneous information on reputation exchanged among nodes.

A judiciary system inspired trust model, known as Trust-based Exclusion Access-control Mechanism (TEAM) [41], has been proposed and is made up of two-tier modules named *local* and *global* context. The local context consist of nodes (i.e. witnesses) that collect behavioral information of their one-hop-neighbours (i.e. defendant) based on self-observation (using promiscuous mode of listening) and recommendations from peer-trusted-nodes. The collected trust level information will then be passed to the global context module, consisting of jury nodes, that will further evaluate the evidence using a voting mechanism based on majority votes. Subsequently, nodes that are found to be malicious/uncooperative, will be punished and denied access to the network. The main goal of TEAM is to provide an accurate exclusion mechanism of misbehaved nodes with low message overhead which was proven based on their analytical and simulation evaluations. However, some of the proposed elements are still obscured in the sense that the trustworthiness of jury nodes cannot be firmly assured prior to getting their opinions. Although the model practiced random selection of jury approach to avoid node collusion, the reliability of information provided by the jury, must be validated beforehand. A mechanism that also utilized the trust model was proposed in [42]. Significant difference of the trust model in this work is that, the model is strengthened with trust features, viz., trust value metrics, packet precision and blacklists. The trust model was implemented in their proposed friendships mechanism such that only friends (i.e. nodes) that fulfilled the trust features' criteria will be fully trusted and used in the route establishment process. Thus, the trust model in [41] may need to consider using trust features and friendships mechanism to strengthen the reliability of the selected jury nodes.

In [43], the trustworthiness of a node is modeled by calculating the weighting average of a particular observed node performing some network tasks over the course of accumulated observations. The accuracy of trust value is strengthened by integrating the model with link quality information measured using statistical model. Although the model was developed for securing routing protocol against several malicious attacks, but it might as well be adopted by any reputation schemes to evaluate trust and combat node collusion. An approach to evaluate the compatibility of existing trust metrics with trust-based routing protocols using routing algebra has been proposed in [44]. The analysis performed in this work contributed to the discovery of several conditions under which the proposed trust-based routing protocol works correctly and optimally from the aspects of such as diversity and absorptive. Also, this work presented cases of where certain trust metrics usage would induce conditions like routing anomalies and inference problem that should be avoided in any trust-based routing protocol design; including reputation-based scheme.

3.1.3. Hybrid Scheme

As an alternative to the two types of incentive mechanism, the hybrid scheme was introduced, featuring the advantages of both credit payment and reputation schemes. The issues that have led to the creation of hybrid schemes include *even distribution of credits*, *challenges of having a central agent in volatile network environments like MANET*, *minimizing processing burden in nodes if a decentralized architecture is adopted*, and *dealing with node collusion*.

In what follows, these proposed hybrid schemes attempt to address the aforementioned issues. A hybrid scheme named hybrId inCentive mechAnism for coopeRation stimUlation (ICARUS) [45] was proposed to improve unfairness distribution of credits among distant nodes by utilizing reputation estimation to control credit exchange. ICARUS inherits some features from a reputation scheme called DARWIN [46]. This scheme relies on a central agent, named ICARUS Credit Accounts Service (ICAS), to manage all credit transactions by acting as reward coordinator, and eventually determine a selfish node. However, it was not explained how efficiently can ICAS collect the needed information. Nodes are assumed to be willingly bounded to follow cooperative policy endorsed by the ICAS, which in reality is difficult to achieve in ad hoc networks due to the autonomous nature of the nodes. In addition, reliance

on a central agent and acknowledgment packets dissemination processes are computationally costly which can incur high communication overhead. These limitations were noted but not rigorously analyzed.

ARM [47] is another hybrid scheme based on the combination of reputation and credit systems. Unlike ICARUS, it does not rely on a central agent to manage credit transactions. Instead, each node has to organize credit payment among corresponding peer nodes based on the value of their reputation. A significant difference between ARM and non-hybrid schemes with the same technical approach is that the load of storing reputation information is assigned to nodes that are static or in low mobility state and are assumed to be relieved from relaying tasks. These nodes act as reputation managers to save mobile nodes that function as relays from being burdened by heavy computational loads. However, the authors did not clarify how certain nodes are regarded as static or low mobility, thus are appointed as reputation managers. Although such an approach may have reduced the heavy processing burden on nodes, freeing some nodes from relaying tasks may not be a good way of utilizing resources.

A scheme named reputation-based credit mechanism (RCM) [48] was introduced with the aim of using the reputation level of a node to estimate the risk of payment prior to submitting it to a central agent called Settlement Centre (SC). Although this work has been able to propose an efficient way to balance the amount of charging and rewarding cost, it is only applicable to network environments with small number of selfish nodes.

3.2. Punishment-based Mechanism

Punishment-based approach penalizes nodes that behave selfishly by isolating them from a routing path or denying them any communication service request. Punishment is the signal to such nodes that selfish behaviour does not benefit them. Besides being applied when a selfish node is detected, punishment is also the next step to be taken after node is rated with low reputation value. Thus, reputation and punishment or payment schemes always work hand in hand, and some of the above described work on reputation mechanisms can also be classified as a punishment scheme such as in [30, 31, 32]. For payment schemes, the punishment is more subtle in such a way that when a node is running out of credits due to constant act of selfishness, it will lose the ability to forward its own packets.

Many existing work on punishment-based scheme applied the popular game theoretical Tit-for-Tat (TFT) strategy to punish selfish nodes [49, 50]. In TFT strategy, a node will take similar action (i.e. cooperative or selfish) as what the other node has done previously. The strategy is played in such a way that a node will be cooperative in the first game stage and subsequent action depends on the opponent's behaviour in the preceding stage. A packet forwarding based game model implemented in wireless ad hoc networks was proposed by [51]. This study looked into possible situations on whether or not cooperation in wireless ad hoc network can emerge without the aid from incentive mechanism. In order to analyze such state, the authors utilized a game theoretic model based on Tit-for-Tat strategy, forwarding game and repeated game. The connectivity among nodes is illustrated by strategizing network topology and routing path based on dependency graph, while cooperation is determined based on nodes' willingness to forward packets for others. Simulation results showed that some portion of nodes can cooperate naturally, thus an incentive mechanism to stimulate cooperation is not needed.

A rigorous study on how to stimulate cooperation in a wireless multicast network using game-theoretic approach was done in [52]. Three main important aspects of cooperation stimulation have been proposed in this work: the modeling of cooperative aspect using infinite repeated game concept to determine the optimal cooperativeness power level, the introduction of punishment based mechanism based on Worst Behavior Tit-for-Tat (WBTFT) strategy and the proposal of a realistic interval estimation mechanism when the result of node behavior monitoring is imperfect. The key concept of cooperation stimulation strategy in this study was in monitoring results, where a node will act equally bad toward a deviating node as a punishment for the act of selfishness (WBTFT), thus reducing the payoffs of selfish nodes. With this mechanism implemented, nodes are theoretically expected to cooperate in order to gain higher payoffs. This theoretical analysis was validated with simulation results and proven to achieve sub-game perfect Nash equilibrium (NE) under certain conditions. In order to achieve realistic cooperation, the authors considered the case where the monitoring results are imperfect due to external factors like noise and interference, and proposed enhancement of the interval estimation to achieve average payoffs that are almost equivalent to that of perfect monitoring output.

Another variant of the punishment strategy is based on Grim Trigger which was applied in [53]. Nodes that follow the grim trigger strategy starts the game by being cooperative and will continue to cooperate until at least one of its opponents deviates from the cooperative mode. When this happens, nodes will stop being cooperative in the

subsequent stages. In the next section, we will extend our discussion on game theory and how it has been used as a tool to analyze cooperation stimulation mechanisms.

3.3. Using Game Theory to Model and Analyze Cooperation Stimulation Mechanisms

Game theory is a mathematical tool originating from economics that can be used to analyze interactive decision-making processes among different rational agents (i.e. decision makers) [54, 55, 56] whereby, it predicts the exact or most likely decisions to be made. It has become a universal tool incorporated with cooperation strategies proposed for wireless multihop networks. A game theory model for wireless networks has three main components: (1) players (decision makers, viz. nodes), (2) actions (choice/strategy e.g. power level setting, packet forwarding, flow control parameter, etc.), (3) preference (utility function/payoffs i.e. high SNR, low BER, low power, throughput, delay, etc.) [57]. In a game, each player has its own preferred strategies that are initiated in response to other players' strategies in order to gain reward. The same scenarios can be mapped to the way nodes in wireless multihop networks communicate, in which each node's actions are heavily dependent on whether or not it will gain payoffs as a result of performing certain actions (i.e. cooperation). Considering that all nodes expect payoffs by being cooperative, this is where game theory can be utilized to reduce selfishness and encourage cooperation.

Table 1 summarizes several existing game theoretical approaches (including those discussed in previous section) addressing the issue of selfishness in wireless multihop networks, where some important key points have been highlighted. In order to solve the problem of selfishness, these schemes have implemented incentive- or punishment-based mechanisms and incorporate them with game theory elements like repeated game, prisoner dilemma, Tit-for-tat strategy and Nash bargaining. These elements were utilized to analyze the conditions in which cooperativeness can occur, such that nodes can be naturally encouraged to cooperate, while knowing that they will not gain payoff by being selfish. Although game theory can be applied to solve cross layer issues [55, 58], the work presented in Table 1 concentrates mainly on cooperativeness issues in network layer like routing and packet forwarding.

For example, in [59], the work focused on resolving the issue of nodes silently drop control packets during route request (RREQ) session in ad hoc networks. Thus, they implemented a monitoring mechanism during route discovery, but not during data packets transmission after route has been established. The basic idea is that, the amount of RREQs relayed should almost be equal to the number of nodes of the same neighborhood. Otherwise, it simply proves selfish activities are on-going. If a node does not reach a pre-determined threshold value of relayed RREQ, it is regarded as selfish and will be punished. In order to avoid false monitoring detection, the algorithm is strengthened with repeated prisoner dilemma game. A significant contribution of this work is that the authors did not use promiscuous listening and indirect communications to monitor node behaviour in order to save energy. Instead, they used a non-complex fully distributed monitoring algorithm to detect and punish selfish nodes. In [60], a mechanism was proposed to model a cooperation strategy among nodes and access point (AP) in a cooperative wireless network. They concentrated on how to ensure each user (source and relay) can have symmetrical benefits of helping each other in the network. Hence, a symmetrical system model based on Nash bargaining solution has been proposed. In this model, two nodes that can both act as a source and a relay can bargain with each other on when or how much bandwidth they can provide for cooperation to take place. In the bargaining process, if both nodes can reach a satisfactory condition, they will cooperate. Otherwise, they will operate independently which does not benefit the network in the end.

A unique incentive-based mechanism was proposed in [61] that aims to challenge the norm of cooperation stimulation approaches by proving that full cooperation of nodes is not necessary, given certain unavoidable condition in the network. Hence, this work proposed a power control mechanism to exploit the existence of seemingly non-cooperative nodes but actually having unintentional factors like energy depletion that restrict them from being cooperative. The goal is to determine an optimal point of cooperation where a certain submaximal forwarding rate is sufficient, that allows a particular node to temporarily suspend its effort in order to restore its energy, and yet not be accused as selfish. In this way, node is expected to be naturally willing to cooperate as it knows for sure that by being optimally cooperative will not jeopardize its resources. The novelty of this work is undeniable, however, deeper considerations need to be investigated as many real network scenarios with more challenging conditions have not been considered. For instance, it is still hard to distinguish liar nodes from the genuine nodes that have stopped their efforts due to optimal forwarding point having been achieved. Hence, further verification is required to ensure that the proposed mechanism can indeed work efficiently.

In term of efficiency measurement, while Pareto optimal (a condition where one player/node impossibly gains payoff without making at least one other player/node worse off) is an option, most schemes utilized Nash equilibrium

Table 1: Game Theoretical Approaches

Author	Cooperation Mechanism	Focus Problem	Contribution	Game Theory Element	Efficiency Validation
Felegyhazi *et al.* (2006) [51]	–Topology control –Incentive mechanism (certain condition only)	To prove that under certain conditions, cooperation can exist without incentive mechanism	Introduce dependency graph concept	–Cooperative model –Tit-for-Tat strategy –Forwarding game –Repeated game	Nash equilibrium
Huang *et al.* (2007) [59]	–Punishment-based	Detecting selfish nodes during route discovery	Selfishness detection and punishment algorithm	–Repeated prisoner dilemma	Nash equilibrium
Zhang *et al.* (2008) [60]	–Incentive mechanism (bandwidth allocation)	Unfairness of benefits distribution among cooperative nodes	Symmetrical system model	–Cooperative game model –Nash bargaining solution	Pareto-optimal
Lee *et al.* (2008) [62]	–Incentive mechanism (payment-based)	Fairness problem in forwarding data	Introduce virtual currency as reward	–Complete information model –Unrepeated non-cooperative game	Nash equilibrium
Ng and Seah (2010) [50]	–Lightweight punishment-based	Unstable network behaviour with the existence of selfish nodes	Propose a protocol that is robust against selfish nodes	–Cooperative game model –Infinite repeated game (Aoyagi's game) –Tit-for-tat strategy –Imperfect private monitoring for dynamic Bertrand oligopoly –Grim Trigger strategy	Nash equilibrium
Zhong and Wu (2010) [63]	–Incentive mechanism (payment-based)	More than one node cooperatively misbehave to gain incentive by cheating	Cryptographic scheme to prevent collusion and profit transfer	–Complete information model –Repeated game	Strong Nash equilibrium
Niu *et al.* (2010) [52]	–Incentive mechanism (punishment-based)	Cooperation enforcement using imperfect monitoring	Improvement of imperfect monitoring	–Infinite repeated game –Folk Theorem	–Absolute fairness –Pareto optimal
Sun *et al.* (2013) [61]	–Less stringent incentive mechanism	–To achieve transmission efficiency with the existence of non-cooperative nodes –To identify non-cooperative nodes due to unwitting condition like energy depletion and node mobility	–Exploiting non-cooperative nodes to ensure communication operational availability –Propose power control mechanism to find an optimal point where full cooperation is unnecessary to avoid energy wastage	–Infinite repeated game –Dynamic repeated game	Subgame Perfect Nash equilibrium (SPNE)

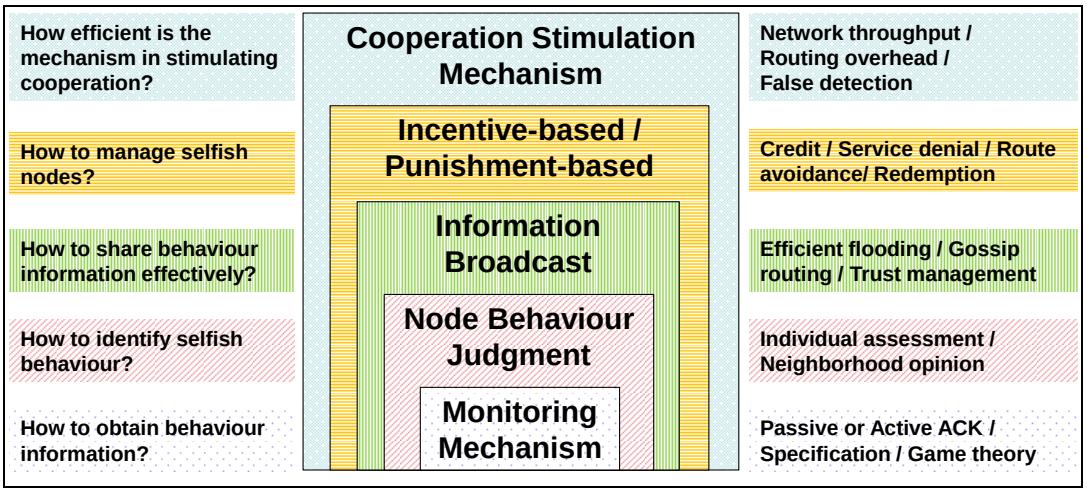


Figure 3: Structure and Components of Cooperation Stimulation Mechanism

(NE) to validate the efficiency of the game theoretical elements in used such as [50, 62, 63]. A perfect NE is achieved when all nodes stick to their preferred strategies and do not change even after considering other nodes' strategies. By assuming that all nodes are rational, nodes will not deviate from steady state game strategies because their payoff cannot be increased. Thus, in the case where cooperativeness is chosen by players as strategy, it is expected to be maintained throughout the whole stages of a game. However, in order to achieve NE in real wireless multihop networks, major assumptions are required including unrealistic ones. For example, it is assumed that nodes can obtain complete information about other nodes' strategies, without considering the feasibility of getting such information in real networks. In many cases, they have to rely on promiscuous listening to implicitly obtain other nodes' actions such as in [51, 46]. In addition, most work modeled game interactions for static nodes only where the occurrence of repetitive game is highly assured. In reality, it is challenging to ensure that a game can be played repeatedly even for a static topology due to problems like communication disconnectivity and busy channels. Hence, the proposed solutions may not be flexible enough to cater for the dynamic nature of nodes in wireless multihop networks. These scenarios show that significant challenges need to be taken care of before game theory can become an efficient tool for cooperation stimulation in real networks.

4. Structure and Components of Cooperation Stimulation Mechanisms

The overall structure and basic components that compose cooperation stimulation mechanisms/schemes are illustrated in Figure 3. Basically, there are five major components involved, whereby each component provides solutions for arising questions listed on the left side-bar of the structure by using available approaches listed on the right side. The two upper components have been discussed in Section 3 and summarized in Table 3 with highlights on general strength and flaws of each cooperation-based category. The lowest layer denotes the most fundamental component that should be present, which is the monitoring mechanism used to observe node behaviour. The behaviour information will be evaluated using node behaviour judgment approaches denoted in the upper layer, whereas, in the case where information needs to be broadcast, approaches presented in the third layer take part. The bottom three layers are elaborated further in the following subsections.

4.1. Monitoring Mechanism

The process of observing and detecting node behaviour plays important roles in ensuring the effectiveness of the other components. However, getting accurate evaluation of a node's behaviour is challenging due to several factors that may be derived from either false judgment by observer or weaknesses of the monitoring methods used. Issues that are being addressed include inaccurate accusation by a group of colluding nodes, insufficient behaviour evidence

and so forth. Some of the aforementioned problems have been addressed in current research by improving some deficiencies in obtaining behavioural evidences such as [64, 65]. Existing work on improving this element have mainly focused on selfish behaviour detection that resides at network and medium access control (MAC) layers. At network layer, selfishness is demonstrated by nodes in the form of route discovery refusal, reluctance (drop or delay) to forward packets, route exploitation (using established route initiated by other node for own data transmission), excessive idle state and unfair provisioning of services. On the other hand, selfishness at MAC layer can be observed in the form of unfair contention channel access, backoff manipulation and false announcement of signal's state. In this paper, we focus on discussing selfishness occurring at network layer where aspects like the monitoring technique used will be covered. In general, a selfish behaviour that occurs in a network layer can be observed using four main approaches: (i) passive acknowledgment, (ii) active acknowledgment, (iii) specification-based approach and (iv) game theory of perfect/imperfect public/private monitoring.

4.1.1. Passive Acknowledgment

Passive acknowledgment, also known as implicit acknowledgment, is the most commonly utilized method to observe node activities in wireless communication networks where nodes run in promiscuous mode of operation – a feature that is widely available in existing wireless communication technologies, such as, IEEE 802.11 or WiFi [66]. When this mode is turned on, a node is capable of overhearing any transmitted packets by neighbouring nodes within its transmission range to determine their forwarding behaviour as introduced by Marti *et al*. [27] in a scheme called *watchdog*. The watchdog mechanism has been widely applied in many work, especially those related to misbehaviour detection and cooperation stimulation approaches. Although the mechanism could record forwarding activities by nodes at reasonable rate, it is with *assumption that channels are reliable*, whereas in reality, this monitoring mechanism only works well in an ideal environment that features collisions-free communication channels, genuine misbehaviour reports and reliable transmission power. A significant advantage in using this mode is that the node does not need to rely on information provided by other nodes in order to evaluate the behaviour of neighbouring nodes as information can be obtained locally by listening to forwarding activities, thus reducing risk of getting false reports. Nonetheless, it has been widely used by many existing work as shown in Table 3 for its significant success to provide reasonable sufficient information despite the aforementioned trade-offs. This is further strengthened by other proposals to enhance the weaknesses posed by watchdog mechanism, such as [67, 68, 69], that show the viability of this method.

Another issue that has been emphasized when utilizing this method is *high energy consumption* that a node has to endure due to occasional process of interface switching. Energy consumption is an important factor to be considered since a monitoring technique that can cause a node's energy to deplete easily may not be a worthwhile option. Similar concern also implies the storage overhead issue where an observing node must allocate some buffer to store the observed information that may burden its computing resource. The combination of energy and storage usages causes a watchdog node to be burdened with high computational tasks when performing the watchdog function. As a node may be overloaded with other communication tasks, a technique that is as lightweight as possible should be adopted in order to maximize a node's lifetime, thus prolonging its ability to function in the network.

Privacy is also another issue to be considered when dealing with promiscuous mode of operation. The capability of overhearing the activities of neighbouring nodes within the same wireless transmission range will also enable a node to get information like node's identity, source/destination address and other routing/forwarding details. Although the reason of collecting such information is for a good cause (i.e. to detect selfish node), the privacy of the observed node may be violated, in which case security issues might arise. Disclosing a node's private information may cause the node and the network to be prone to vulnerabilities like stolen identities, denial of service and other illegal acts. The question is, *how do we utilize the advantages of promiscuous listening despite its weaknesses?* Hence, researchers who intend to use promiscuous mode as an observing technique must find acceptable (if not optimal) balance between those aforementioned aspects such that behaviour information can be obtained at reasonable trade offs. Due to the issues in passive acknowledgment, other work promote alternative ways to monitor node behaviour by using active acknowledgment.

In term of *routing protocol* used to obtain implicit information, source routing such as Dynamic Source Routing (DSR) has been the most chosen underlying routing protocol by existing cooperation stimulation schemes such as [27, 28, 29, 31, 30, 46]. One reason is due to its built-in optimization of promiscuous listening. With DSR, nodes are able

to obtain complete information of an established route, like number of hop counts stored in packet's header. However, other routing protocols such as Ad-hoc On-Demand Distance Vector (AODV) can also use the promiscuous interface as the integration of the interface with the protocol has been established and is utilized widely. Schemes that rely on AODV routing protocol and utilized promiscuous mode are such as [41, 42].

4.1.2. Active Acknowledgment

In contrast to the passive acknowledgment approach, active acknowledgment does not rely on MAC layer to implicitly obtain information on node behaviour. Instead, it uses explicit acknowledgment from peer nodes (either in end-to-end or hop-by-hop fashion) by transferring acknowledgment (ACK) packet for any successfully received packets.

End-to-end acknowledgment

In this approach, the destination node is required to send an ACK packet back to the source node to notify that it has successfully received the packet. If the source node does not receive an expected ACK packet within a specified time, it will consider the data packet to have failed to reach the destination. In [34], a general framework on reliable routes and cooperation enforcement policy was proposed to increase performance and reliability of ad hoc networks. A reliable route was determined based on its reliable index, whereby every detected dropped packet event on a particular link will reduce the link's index. When the reliable index drops beyond the minimum threshold, the route will be avoided. The dropped packets scenario is detected based on end-to-end acknowledgment whereby the destination node will send an ACK packet back to the source node upon successfully receiving a packet. A significant weakness in this work was the assumption of the visibility of every link's reliable index to all nodes along the path. The work in [35] also used the end-to-end acknowledgement method to evaluate the behaviour of neighbouring nodes. In this scheme, a reputation value is assigned to the next hop neighbour alone, not all nodes along the route. The evaluation of a node behaviour in [36] was done by relying on TCP acknowledgments. If a packet successfully arrives at the intended destination, the destination node will send an ACK back to the source. Upon receiving a successful ACK, each node along the path will increase the reputation index of their neighbouring nodes. Deduction of reputation index happens when a node realizes that its neighbour did not forward an ACK back or it forwarded a retransmission of same data packet, which denotes a selfish behaviour.

Hop-by-hop acknowledgment

A similar routine is also applied for the hop-by-hop acknowledgment scheme, except for the length of path that ACK packets need to travel is shortened, whereby other than destination node, intermediaries are also responsible for generating and sending ACK packets back to source node. To alleviate the problem of accusing the whole route consisting of multiple nodes, which causes unnecessary punishment towards innocent nodes, Balakrishnan *et al*. [37] proposed a scheme named TWOACK. Unlike any end-to-end acknowledgment scheme, this scheme works by requiring the node located two hops away from the original sender or other forwarder to send an acknowledgment packet back to the sender upon receiving a data packet. If the waiting-for-ACK-node does not receive any ACK packet within a specified waiting time, the reputation value of the next hop link decreases and when the value drops to a certain threshold, the link is marked as misbehaved and would be avoided in the next routing session. This method helps to detect specific distrusted link rather than punishing the whole route, thus reducing false accusation. In order to reduce traffic congestion due to overwhelming transmission of ACK packets, the authors also introduced an S-TWOACK (Selective-TWOACK) scheme. The S-TWOACK scheme works by grouping a set of data packets' information received from the same upstream link and compile them into one TWOACK packet to be sent back to the source or forwarder, as a notification of successful packet reception. Both TWOACK and S-TWOACK schemes were later improved with the introduction of 2ACK scheme proposed by Liu *et al*. [38]. In the 2ACK scheme, the 2ACK packet was enhanced with an authentication mechanism using one-way hash chain to preserve the authenticity of the packet from forging attack. In addition, the routing overhead in the scheme is reasonably low as the acknowledging process only involves part of data packets instead of all the packets. However, the amount of partially acknowledged packets must be kept within an acceptable ratio to avoid false report.

Having schemes that utilize acknowledgment for shorter portions of an entire route has helped in reducing the number of nodes that may be falsely accused as misbehaved. However, such an approach does not outperform the

end-to-end acknowledgment technique in detecting a misbehaved node. Even a short link marked as "misbehaved" may still contain cooperative nodes. Thus, more misbehaved links need to be detected in order to accurately identify a misbehaved node. This would require significant evidence gathering to come out with concrete judgment. In addition, the efficiency of this method is at the expense of high communication overhead due to frequent transmissions of ACK packets in the network. This is especially true for schemes like 2ACK where every two-hop-away nodes are required to send an ACK packet back to the sender in order to acknowledge packet reception, thus, increasing the network traffic that could lead to congestion. Another significant weakness in the schemes that utilize end-to-end or hop-by-hop acknowledgment is that false positive is likely to happen such as in the case where destination node does not generate ACK back to the source or the ACK packet itself is dropped by any node along the way, a misinterpretation of selfish behaviour could easily occur. In addition, any reliance on TCP ACK makes it unsuitable for transmitting the packet using UDP, which can lead to higher communication overhead. In order to stimulate cooperation, nodes should not be burdened with extra forwarding tasks than what they already have.

Probing

Another form of active acknowledgment is based on *probing*. In this technique, a node monitors another node's behaviour by sending out probing packet to any neighbour that is one hop away from the monitored node and expects an acknowledgment report from that neighbour node. For instance, node A wants to check node B's forwarding behaviour, so it needs to send a probing packet to node C which is one hop away from node B. Assuming that node C is well-behaved and has node B's forwarding behaviour information, ideally it would send an acknowledgment packet back to node A to report on node B's behaviour. Upon receiving the acknowledgment packet, node A gets confirmation on node B's forwarding behaviour based on the information sent by node C. Examples of work that have applied the probing technique are [70, 71]. However, schemes that rely on using packets to probe have some weaknesses, namely, the dependence on other nodes to verify the behaviour of certain nodes may lead to false judgment in the case where the node replying to the probing packet gives a false report. In addition, in reality it is hard to be sure of whether or not a probing packet can be sent to any node that is one hop away from the observed node. In the case where no one-hop-neighbour of the observed node is visible, there is nowhere to send the probing packet .

4.1.3. Specification-based Approach

Another variance of behaviour observation method is using the specification-based approach, which is a method of monitoring the behaviour of a certain object and comparing it with a predetermined specification or policy that the object needs to follow, and check whether or not that object abides by it. Specification-based approach has been used as an alternative to anomaly detection in identifying behavioural pattern of nodes in wireless multihop networks whereby focus has been given on creating specifications for routing protocols. In the work by Wang *et al*. [72], the authors proposed a specification or policy for the route discovery process in AODV routing protocol that nodes need to follow by introducing local routing instance (LRI). LRI is a set of ideal transmission processes that happens during a route discovery session and needs to be completed by a monitored node. In order to keep track of possible behaviours of every monitored node, the observing node is guided by a finite state machine (FSM) model. The FSM model acts as a guideline for a local observing node by evaluating sets of possible sequence of behaviours that might be shown by any monitored node. Through these sequences, node behaviour can be identified based on their ability to reach the final state of FSM, which is to complete LRI. Selfishness is determined based on number of final states that a node has failed to reach and has gone beyond certain threshold value. Earlier work on specification-based approach supported by FSM model was proposed by Tseng *et al*. [73]. However, this work did not attempt to detect selfishness, but focused more on malicious behaviour detection launched by attackers. The proposed scheme was the first to utilize specification-based approach and has been embedded in an intrusion detection system to detect attack in AODV routing protocol. A similar variant of FSM-based intrusion detection scheme for AODV was proposed by Ye and Li [74] where classification of several attacks on AODV routing protocol has been made. This technique has been further applied in many other existing work such as [75, 76].

4.1.4. Game Theory of Perfect/Imperfect Public/Private Monitoring

Apart from being applied in many existing punishment-based mechanisms as discussed earlier, game theory has also been utilized in observing node behaviour for its capability to provide monitoring analysis model. Several ex-

isting work on detecting node misbehaviour have implemented game theoretical observation components named perfect/imperfect public/private monitoring as alternatives.

Perfect public/private monitoring

Perfect monitoring is a condition where players of a particular initiated game are able to directly observe other players' actions [77, 78]. Subsequently, the entire results (denoted by s^*) obtained from the decision making process by each player are also visible to every other players. Equilibrium is achieved such that no player is known to have deviated from s^* to maximize its own payoff which means that every player will always play a fair game. The observed deviation is the element that can be used to determine consequent actions such as punishment. In the wireless multihop network context, it is equivalent to a situation where each node is able to observe other nodes behaviour or strategies at the end of each stage of the game or history of behaviours in previous rounds, in the case of repeated games. This model is also known as perfect public monitoring where signals (i.e. actions) produced by any node are publicly observable and shared with other nodes in the same network. In such a case, the signal $\omega = (a_1...a_n)$ and $\omega \in Y$ where a_i are the actions taken by each player (Y) at every stage of game. In real wireless multihop networks scenarios, it is not practical to apply the perfect public monitoring concept due to uncertainty nature of node behaviour in the network where it is difficult to predict that node behaviour is consistent for every round of game. In other words, it is hard to obtain perfect observatory of node actions where accurate conclusion can be made to perform subsequent actions. Otherwise, assumption has to be made such that every node has the complete information about other node behaviours, which is unrealistic.

Imperfect public monitoring

The difficulty of interpreting ambiguous signals can be alleviated using repeated games of imperfect public monitoring [79, 80] in which ω is a random variable. This method introduces observation based on random public signal which is correlated with players' actions in a game, whereby the signal is assumed to be consistent. In imperfect public monitoring, players cannot directly observe the actions taken by other players, but may monitor the random signals produced. The signals can be considered as implicit signs of the actual actions taken by players. For instance, in tacit collusion under demand fluctuations by Green and Porter [81], two firms that are competing with each other may not be able to observe the quantities of products that the other firm has produced. However, they can observe the market price advertised that may reflect the information of product quantities, whereby low price may indicate that the quantities of production are high. In the wireless multihop network context, this is similar to a scenario where an observing node may be able to predict other node behaviour based on some indicator of overall network performance such as network goodput. For example, the work done in [82] applied the imperfect monitoring approach to encourage nodes in ad hoc networks to participate in packet forwarding by observing public signal levels and executing punishments when the level falls below a certain threshold value. In this study, the public signal is indicated by aggregated network goodput such that if nodes do not deviate from the ideal forwarding behaviour, the signal is maintained at optimal level. However, if the signal level falls below the minimum threshold that has been set, which indicates significant node deviation from the game, a trigger point based on Grim trigger strategy is initiated allowing all nodes to drop packets (i.e. entering punishment phase) causing incentive loss for all involved nodes. Thus, in order to avoid losing incentive, nodes are self-motivated to keep the signal at the optimum level by not deviating from the game. Although this kind of strategy seems to work well in encouraging nodes to cooperate, in reality, it is difficult to obtain information on any selected public signal and disseminate them through the network so that all nodes could take the signal as reference of the intended behaviours in forwarding packets. In addition, this kind of approach executes punishment that will affect all nodes in the network, while the real culprit still cannot be detected. Such punishment method may actually waste network resources due to unnecessary packet dropping by cooperative nodes when the punishment stage is triggered. The real challenges in applying imperfect public monitoring to stimulate nodes cooperation in wireless multihop network can be highlighted as follows:

a. Determination of public signal must consist of these properties: (1) it represents the strategies played by each node; (2) it must be mutually related to the combined strategies of all nodes; and (3) all nodes acknowledge the signal after each stage of game;

b. Nodes must be willing to unanimously select and share the same random public signal as their reference points;

c. Signal must be sufficiently identified in order to execute punishment targeted to deviators; otherwise every node may suffer from unnecessary punishment;

Considering the above mentioned challenges, it is obvious that the existence of such random public signal is very rare in wireless multihop networks. Besides, in order to identify the signal, a lot of coordination and information collection process in the network are required, which could lead to high traffic and communication overhead.

Imperfect private monitoring

In order to counter the above-mentioned issue, another game theoretical monitoring model named imperfect private monitoring [83, 84, 85] was studied. In this model, each action a represents a unique private signal ω where,

$$(a_1, \ldots, a_n) \begin{array}{c} \nearrow \\ \longrightarrow \\ \searrow \end{array} \begin{array}{lcl} \omega_1 & \in & Y_1 \\ \omega_2 & \in & Y_2 \\ \vdots & & \vdots \\ \omega_n & \in & Y_n \end{array} \tag{1}$$

For this imperfect private monitoring model, the action a_i and the signal ω_i are player Y_i's private information and are not observable but may be evaluated based on certain output condition, that is also imperfect. We will discuss an example application of imperfect private monitoring based on the above-mentioned tacit price cutting. In this case, price is not observable and the firm's sales total is the only signal that can be evaluated but it is private information and imperfect due to demand fluctuations. However, this information can be used to predict the hidden actions of other players albeit with a probability of making a wrong decision. Application of imperfect private monitoring method in wireless multihop networks is still in its infancy stage due to difficulties in maintaining the game recursively and the lack of information to continue the game for the next stages.

One such approach that has been applied in monitoring the behaviour of nodes in wireless multihop networks is the work by Ng and Seah [50]. This work adapted a game model that is derived from Aoyagi's game of imperfect private monitoring and communication for Bertrand oligopoly [86]. In general, Aoyagi's game is a repeated game of undisclosed information (product price) and communication (advertisement) among players. Each player would publicly declare their selling price, but can secretly reduce the published price when dealing with customers, that would gradually affect the profit gained by other players. The problem lies in how to observe the privately released signals so that appropriate actions can be taken by other players to avoid further loss. In order to solve the problem, the author in [86] introduced a collusive communication among players where each player chooses a collusive price $(p_i)^*$ and eventually reveal their private signals at the end of the collusion stage. Similar communication element has been implemented in [87, 88]. The private signal d is reported in the form of either 0 or 1 indicating low or high signal respectively that is determined by comparing with threshold value $(m_i)^*$. The decision on whether or not the communication remains in collusive mode or turn into punishment mode is highly dependent on the uniformity of the reported private signals by every player. As opposed to imperfect public monitoring where the observation signal obtained does not necessarily reflect the real action of each player, imperfect private monitoring on the other hand does provide more accurate signal. However, it is difficult to implement as there is still no guarantee of obtaining a genuine signal. Rationally, each player would still possess a likelihood to lie (i.e. give false report) but equilibrium is built in such a way that incentive will be given when genuine reporting is maintained or else punishment will take place.

4.2. Node Behaviour Judgment

Judging a node's intentions by observing its behaviour can be very challenging especially in a wireless network, where information can be lost or altered by the environment. In this section, we examine the various techniques used to assess a node's behaviour so that the outcome can be used to determine whether a node is cooperative or not.

4.2.1. Local vs. Global Information

In order to gain the information on node behaviour, it is important to identify the source of behaviour information i.e. whether it should be obtained locally or globally. Local or direct observation means that a node evaluates the

behaviour of other nodes based on its personal experiences and observations. In contrast, getting information globally (i.e. indirect observation) implies that a node gains information on a particular node behaviour based on the external opinions of other nodes to support its evaluation. In this case, information dissemination will most likely occur in the network in order for nodes to exchange information. As shown in Table 3, analysis on information source shows that most payment-based schemes do not apply any behaviour observation methods, unlike reputation-based and punishment-based schemes, due to the nature of these schemes which rely on credit system whereby, loss of credits is regarded as an automatic punishment to selfish nodes.

Local observation is applied in most existing incentive-based mechanism and is considered as a compulsory procedure due to the important need for every node to self-evaluate other nodes prior to getting external information. The difference is in terms of whether or not local observation is exchanged with other nodes in the network and obtained information is supported by global reports. Schemes that rely on local observations only, such as [31], were motivated by the fact that issues in getting global information such as false accusation, unscalable information management and unnecessary overhead due to information flooding are avoided. However, this option is applied at the expense of getting insufficient information about the behaviour of other nodes. On the other hand, nodes that obtain behaviour information based on reports from other nodes are prone to risk of getting false reports, especially when the other nodes collude with each other to mask the real behaviour of a particular node for self-benefits. Hence, the decision of determining the information provider is critical in any incentive-based mechanism for detecting the real behaviour of a particular observed node.

Differences between implementing local and global observation in determining node behaviour in wireless multihop networks are summarized in Table 2. Based on the summary, there are pros and cons in determining the types

Table 2: Local Observation vs. Global Observation

Sources / Elements	**Local Observation**	**Global Observation**
Topology	Could adapt well with dynamic changes of topology	More suitable for static topology
Overhead	Less communication overhead	More communication overhead due to information exchange/distribution
Scalability	More scalable due to behaviour information is viewed from the perspective of a single node and need not be shared or exchanged	Less scalable due to the need for information to be shared across network and to maintain global behaviour information of other nodes
Information Sufficiency	May not have sufficient information on the overall state of node behaviour	Able to collect multiple opinions from other nodes
Node Collusion	No risk of node collusion but false accusation may occur	Higher risk of getting false accusation by colluding nodes

of observation sources between local and global observation for node behaviour evaluation. The choice depends on the efficiency of each method in providing information on selfishness at reasonable trade-offs among elements listed in the table. However, until now, each method still needs to be improved to strengthen the authenticity of behavioural information that are observed and possibly shared across the network.

4.2.2. Monitored Behaviour

At the network layer, two major node functions are routing and forwarding data packets which can be observed and evaluated by an observer to determine cooperativeness/selfishness behaviour. The effort in forwarding packets can be measured using performance metrics like forwarding rate and number of dropped packets. Other factors like dropping probability and wireless transmission error might also be considered to get a more accurate measurement as has been applied in [45, 46]. With that implies, a threshold value is set to determine the level of node's effort as being either cooperative or selfish.

4.3. Information Broadcast

The obtained behaviour information may need to be shared with other nodes to strengthen judgment and get concrete evaluation. The class of reputation-based schemes is among ones that require behaviour information to be broadcast in order to determine the reputation level of a node based on votes from other nodes. This would require efficient techniques to disseminate the information so that it reaches intended destinations correctly. One important aspect is on the underlying routing protocol used. With respect to information broadcast, DSR has more advantage due to the fact that a source node knows the information of other nodes in the entire established route. In addition, nodes in DSR area able to learn and store multiple routes. This means, behaviour information can be shared with large number of known nodes without having to flood and exchange the packets containing such information to anonymous nodes. Unlike DSR, nodes in AODV only know their next hop neighbours. Thus, it has to depend on other nodes to broadcast information to nodes of beyond its channel coverage. Although storage overhead can be reduced, broadcasting information using AODV would cause higher communication overhead. Nonetheless, since both are on-demand protocol, having to flood packets blindly to exchange reputation information is unavoidable. Thus, a pro-active routing approach might be a worthwhile consideration.

In [89], broadcasting and exchanging reputation information have been evaluated based on both on-demand and pro-active techniques. Both techniques were found to have advantages and drawbacks in handling such processes. Although on-demand technique has less communication overhead, but with its establishment being temporary, some information might not be shared in timely fashion. Whereas, pro-active technique is able to broadcast information at any time due to its steady-state readiness, but at the cost of having high network overhead.

4.4. Summary

A comparison of the various cooperation stimulation mechanisms was carried out and the results are presented in Table 3. We identified the pros and cons of each element, together with general strength and flaws of each category of schemes.

5. Open Research Issues

Following the review encompassing essential elements in cooperation stimulation mechanisms, we will further discuss several related issues that are still open research problems in this field. The main highlighted issues are false judgment and node collusion, whereby these problems originated from the inaccuracy in the evaluation of a particular node's behaviour.

5.1. False Judgment

As aforementioned, the most basic procedure to obtain information on behaviour is through the observation of a single node, where the information may be shared with other nodes or kept for self-reference. The accuracy of the information is susceptible to false judgment especially when a node behaviour is judged based on single set of actions (SSA) using metrics like number of dropped packets and forwarding rate. SSA is a condition of when a node observes another node's forwarding effort towards its own requests while disregarding that node's effort towards other nodes' requests [90]. This procedure is applied in most of the existing work, whereby the scenario that is most likely to occur due to this practice is that any packet dropping activity (i.e. above certain threshold) by the observed node can be regarded as selfish, which may not be assessed sufficiently. This means that it is not always fair to evaluate a node's effort based on SSA since the observed node may have constraints in fulfilling the request due to other problems, like having to serve heavy incoming traffic.

Apart from having the fairness issue, the lack of adequate information as a consequence of the SSA approach is also a key factor in the reliance on global reports. Commonly, this process has to be done in order to gain assurance as to whether or not the same observed node exudes the same behaviour, as evaluated by other nodes in the network, based on the number of majority votes. However, since the global report is formed based on the information collected from a group of observing nodes that also utilizes SSA, the information may not accurately reflect a particular node actual behaviour, which leads to false judgment. Having said that, the problem of false judgment actually has a cyclic effect, as shown in Figure 4. When a local node requests for global report which is based on the majority of votes cast by other local nodes, the authenticity of the behavioural information may already be contaminated by several

Table 3: Summary of Comparison

Type	Monitoring Mechanism	Information Source (Local VS Global)	Punishment Scheme	General Strength and Flaws
Credit-Payment Scheme (CPS) Nuglets [14,15,16] Sprite[17] Adhoc VCG[18] COMMIT [19] Express[20] RACE[21] Micro-Payment[22] Charge-Reward[23] TRIPO[24] FESCIM[25] CASHnet[26]	**Not Available** [14-19][21-26]	**Not Available** [14][16][17][18][19]	**Not Enforced** [14-18][21-23][25-26]	**Strength** - Credits as incentive motivating node to cooperate **Flaws** - Mostly, selfish node is not detected - High communication and processing overhead - Bottleneck - Storage overhead - Unfair share of credits distribution due to node location - Reliance on costly tamper-proof device
	Pros: - No monitoring overhead - Less energy consumption ***Cons:*** Exact selfish node is not detected	- Nodes are not bounded to observation task to detect selfish node. - Mainly rely on credit transactions to motivate cooperative behaviour.	***Pros:*** Less processing overhead ***Cons:*** Undetected selfish node can get away from network tasks.	
	End-to-end ACK [20]		**Mass Enforcement** *Denial of service* [19][24] *Certificate retraction* [20]	
	Pros: Verification of node's effort is strengthened ***Cons:*** Communication overhead		***Pros:*** Node vindication ***Cons:*** False judgment – periphery node less chance to collect credit	
Reputation Scheme (RS) Watchdog[27] CONFIDANT[28] CORE [29] SORI[30] OCEAN[31] HEAD[32] LARS[33] Performability[34] Malicious Counter[35] Node Isolation[36] TWOACK and S-TWOACK [37] 2ACK[38] SDA[39] TEAM[41] Trust-based[42] DARWIN[46]	**Promiscuous Mode** [27][28][29][30][31][32][33][39][41][42][46]	**Local Observation** [27][28][29][30][31][32][33][34][35][36][37][38][39][41][42][46]	**Mild Enforcement** *(Path avoidance)* [27][32][37][38][42]	**Strength** - Motivate node to increase reputation level by being cooperative - Strengthened behaviour evaluation by using voting mechanism - Unsusceptible to false judgment by small group of cheaters **Flaws** - Prone to false accusation by large group of colluding nodes - Complex trust management design in large topology - High resource consumption and communication overhead
	Pros: - Self-evaluation - Less false report, unless intentionally faked ***Cons:*** - Unreliable channel - High energy consumption - Privacy issue	***Pros:*** - Scalable - Less overhead - Adapt with dynamic topology changes ***Cons:*** - False judgment - Insufficient information	***Pros:*** Possible second chance ***Cons:*** Avoided selfish node can get away from network tasks.	
	End-to-end ACK [34][35][36]	**Global Observation** [28][29][30][39][41][42]	**Mass Enforcement** *(Path deletion, denial of service request, node isolation/ blacklisted, denial of access control)* [28][29][30][31][33][34][35][36][39][41][46]	
	Pros: - Not rely on MAC layer - Less ACK packets propagation ***Cons:*** - Punishing whole link - Less false report, unless intentionally faked	***Pros:*** - Strengthen local judgment ***Cons:*** - Node collusion - High communication overhead - Susceptible to false accusation - Less scalable		
	Hop-by-hop ACK [37][38]		***Pros:*** - Punishment motivates node to cooperate in next stage ***Cons:*** - No redemption may cause resource wastage - Possible false accusation	
	Pros: - Detect specific distrusted link ***Cons:*** - High communication overhead			
Hybrid Scheme (HS) ICARUS[45] ARM[47] RCM[48]	**Promiscuous Mode** [47][48]	**Local Observation** [38][39][48]	**Mass Enforcement** *(Denial of service request, node isolation, denial of access control)* [38][39][48]	**Strength** - Credits as incentive motivating node to cooperate - More balanced charge and reward amount **Flaws** - Possibly very high communication and processing overhead due to the hybrid features
	End-to-end ACK [45]	**Global Observation** [38][39][48]		
	Pros and cons similar to RS.	Pros and cons similar to RS.	Pros and cons similar to RS.	

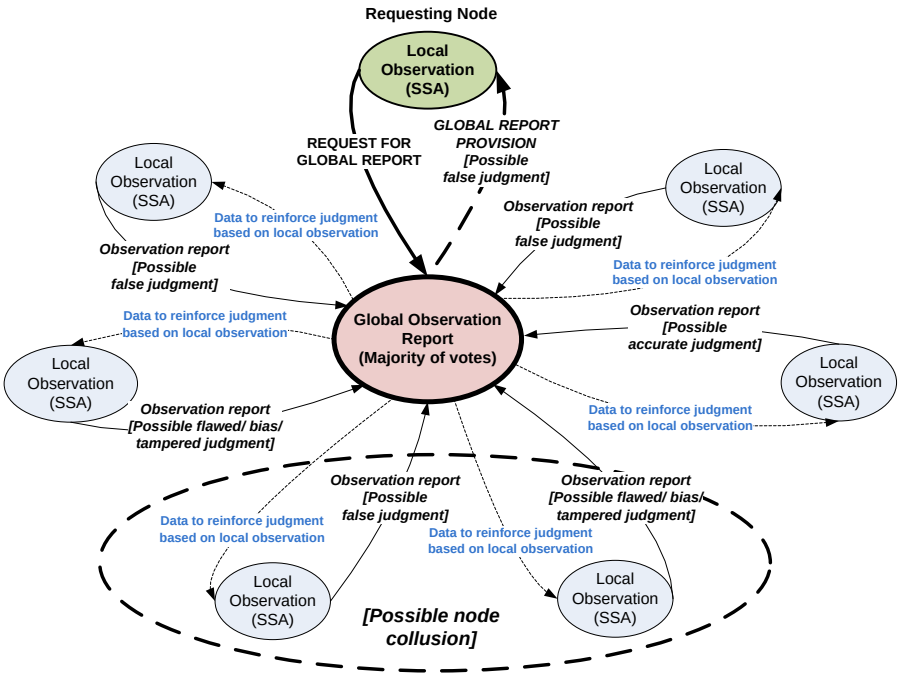


Figure 4: The Circulating Problem of False Judgment based on SSA

factors, such as, biased and tampered judgment. Even with the increasing numbers of voters, a node may only obtain information on selfishness or cooperativeness based on highest portion of votes, while the false judgment problem may still be circulating within the loop. This is because every single observing node has the authority to judge a particular node behaviour based on their own stochastic perceptions by using SSA. Thus, the SSA approach needs to be reassessed where the reliability of the observed information by every single node must be guided by a more efficient mechanism based on policies and/or agreed criteria. The element that needs to be highlighted and focused here is the need to obtain the information on how cooperative and fairly a node's effort is towards different arriving requests, as promptly and accurately as possible. Thus, the aim is to reduce the necessity of having to rely on the global report, as much as possible. As matter of fact, having more accurate local observation information will strengthen the accuracy of the global report if, at certain point, it is deemed necessary by any particular node.

Hence, the accuracy of the common observation routine must be assured, so that an observer node has a smaller chance of making a false judgment. One of the consequences of a false judgment is its effect on global sharing accuracy when the shared information is flawed. Although some reputation mechanisms such as [31] introduced rebound state element by giving a second chance (i.e. redemption period) to a falsely accused node to re-participate in the network, it is more desirable if the reliability of the first-hand information can be guaranteed beforehand. As shown in Figure 3, several elements of the cooperation stimulation mechanism following the behaviour judgment part may be adversely affected as a consequence of having false judgment, and may result in a defective overall cooperation stimulation mechanism. Hence, the behaviour information obtained must be strengthened with some mechanisms that could portray the viability of the reported behaviour which will be further investigated in our study.

5.2. Node Collusion

Node collusion is another issue that is highlighted in this article as depicted in Figure 4. It is not wrong for a group of nodes in a wireless multihop networks to agree on the same behavioural information on a particular node. However, it is not right for them to collude by falsely accusing or praising any node. When this scenario happens, a good node may be unnecessarily punished while a bad node remains undetected in the network. This is a problem that has yet to be addressed successfully in the sense that there is no mechanism to control the reliability of information that the nodes decide to share. Any node requesting information on a particular node's reputation, whether good or bad, would

have to rely on the majority votes. Lack of an accurate method to judge a node behaviour makes it convenient for any node to declare false information because assessment is not guided by any formal metrics or policy.

Intuitively, if nodes are bounded by certain metrics when judging other nodes, where they need to present certain evidences to prove that fair evaluation has been made, the risk of collusion could be reduced. Hence, it is important to provide a mechanism that can ensure the accuracy and reliability of a node behaviour such as a recently proposed method called 'compare and measure selfishness detection' [90]. Above all, the question will return to what type of monitoring techniques should be used in order to obtain accurate information. Given the discussion on the pros and cons of currently available monitoring techniques in Section 4.1, thoughtful consideration must be made prior to making any selection.

5.3. Accuracy

The accuracy of behaviour information is the most fundamental element that has not been fully addressed in existing schemes, which is why the issue of false judgment is still affecting the efficiency of the proposed schemes. Although there exist proposals to improve accuracy from the perspective of physical, MAC and network layers, most come with the assumption that information can be sufficiently collected by using the SSA approach. Even worse, some simply assume that selfish behaviour can be assessed without explicitly stating how such information is actually measured. Hence, deeper investigation needs to be done to improve existing approaches especially SSA, that could provide faster, yet more conclusive behaviour information.

5.4. Scalability

To improve the scalability of cooperation mechanism, it is good to reduce the dependency on centralized approach in managing nodes in the networks. Although having any node appointed as central agent to function as a trust manager or credit administrator would help in coordinating some processes smoothly, but as far as wireless multihop networks characteristics is concerned, it would introduce delays, bottlenecks and overhead when every other nodes need to communicate and submit reports to the agent. Having such dependancy, the more nodes joining the networks, the more hectic the networks would be, leading to scalability issues. However, having distributed approaches also come with some drawbacks as every node may have the authority to make autonomous decision. Hence, nodes that work under distributed mode must be guided with a set of policies, though not as stringent as having to rely on a central agent. Having said that, further investigation on how to exploit the advantageous elements of both distributed and centralized approaches must be carried out.

5.5. Security

Security and cooperation are cross layers issues in the detection of node misbehaviour in networks. While cooperation approaches aim to address the selfishness issue, security approaches on the other hand aim to deal with malicious behaviour. Although selfishness is a subset of malicious behaviour, security mechanisms targeting malicious behaviour may not necessarily be suitable countermeasures for selfishness. But, it cannot be denied that security aspects must also be considered in the design of cooperation stimulation mechanisms, such as, preserving node privacy during monitoring, having authenticated acknowledgment packets and guarantee on non-spoofing of node identity. Hence, there is a need of providing optimal balance between security and cooperation approaches such that elements from both approaches would complement each other to produce the desired outcomes.

5.6. Application

Most existing cooperation stimulation mechanisms have been proposed for general wireless multihop networks but not tailored to meet the specialized requirements of any particular network type. For example, credit-payment scheme with central agent may be more suitable for WSNs where nodes are less mobile, as compared to applications on MANETs where node mobility is high and appointing a central agent may not be feasible for the ad hoc nature of the networks. Thus, there is a need to design a cooperation mechanism that would specifically cater to unique characteristics of different network types.

6. Conclusion

This article presents an in-depth survey on cooperation in wireless multihop networks focusing on cooperation stimulation mechanisms that have been proposed to address the issue of selfishness. Several aspects in the proposed mechanisms like the adopted monitoring and selfishness detection approaches have been discussed in order to identify possible weaknesses prior to finding ways for addressing them. These components are among those presented in the comparative analysis table (Table 3), which play important roles in the development of any cooperation stimulation mechanism. The comparison of the various schemes led to the highlighted issues that will motivate research to find ways in providing accurate measurement of a node behaviour. Having more accurate behaviour measurement is expected to address issues like false judgment and node collusion in wireless multihop networks. To date, these aforementioned issues are open research problems in this area, where proposed solutions still have room for improvement. In view of these challenges, cooperation stimulation mechanisms in wireless multihop networks still require extensive investigations and rigorous research studies, providing abundant opportunities for novel discoveries and new innovations.

References

[1] Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Computer Networks 52(12), 2292-2330 (2008).

[2] Sharef, B. T., Alsaqour, R. A., Ismail, M.: Vehicular communication ad hoc routing protocols: A survey. Journal of Network and Computer Applications 40, 363-396 (2014).

[3] Komali, R. S., MacKenzie, A. B. and Gilles, R. P. : Effect of selfish node behavior on efficient topology design. IEEE Transactions on Mobile Computing 7(9), 1057-1070 (2008).

[4] Yoo, Y., Agrawal, D.P. : Why does it pay to be selfish in a MANET?. IEEE Wireless Communications 13(6), 87-97 (2006).

[5] Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C., Belding-Royer, E. M.: Authenticated routing for ad hoc networks. IEEE Journal on Selected Area in Communications 23(3), 598-610 (2005).

[6] Zhong, S., Li, L. E., Liu, Y. G., Yang, Y. R. : On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: an integrated approach using game theoretic and cryptographic techniques. Wireless Networks 13(6), 799-816 (2007).

[7] Myerson, R. B.: Game Theory: Analysis of Conflict. Harvard University Press, 1991.

[8] Herhold, P., Zimmermann, E., Fettweis, G.: Cooperative multi-hop transmission in wireless networks. Computer Networks 49(3), 299-324 (2005).

[9] Sharma, S., Yi, S., Hou, Y. T., Sherali, H. D., Kompella, S.: Cooperative communications in multi-hop wireless networks: joint flow routing and relay node assignment. In: Proceedings of the 29th IEEE International Conference on Information Communications (INFOCOM), San Diego, CA, 14-19 March 2010, pp. 1-9.

[10] Sharma, S., Yi, S., Hou, Y. T., Kompella, S.: An optimal algorithm for relay node assignment in cooperative ad hoc networks. IEEE/ACM Transactions on Networking 19(3), 879-892 (2011).

[11] Zhang, J., Zhang, Q. : Cooperative routing in multi-source multi-destination multi-hop wireless networks. In: Proceedings of the 27th IEEE International Conference on Information Communications (INFOCOM), Phoenix, AZ, 13-18 April 2008, pp. 1-5.

[12] Lin, Y., Song, J.-H., Wong, V.: Cooperative protocols design for wireless ad-hoc networks with multi-hop routing. Mobile Networks and Applications 14(2), 143-153 (2009).

[13] Khandani, A.E., Abounadi, J., Modiano, E., Lizhong, Z. : Cooperative Routing in Static Wireless Networks. IEEE Transactions on Communications 55(11), 2185-2192 (2007).

[14] Buttyan, L., Hubaux, J.-P.: Nuglets: A virtual currency to stimulate cooperation in self-organized mobile ad-hoc networks. In: Technical Report DSC/2001/001. Swiss Federal Institute of Technology, Lausanne, Switzerland, (2001).

[15] Buttyan, L., Hubaux, J. P.: Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications 8(15), 579-592 (2002).

[16] Buttyan, L., Hubaux, J.-P.: Enforcing service availability in mobile ad-hoc WANs. In: Proceedings of the 1st IEEE/ACM Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC), Boston, MA, 11 August 2000, pp. 87-96.

[17] Zhong, S., Yang, Y. R., Chen, J.: Sprite: A simple, cheat proof, credit-based system for mobile ad hoc networks. In: Proceedings of the 22nd IEEE International Conference on Information Communications (INFOCOM), San Francisco, USA, 1-3 April 2003, pp. 1987-1997.

[18] Anderegg, L., Eidenbenz, S. : Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In: Proceedings of the 9th International Conference on Mobile Computing and Networking (MobiCom), San Diego, CA, 14-19 September 2003, pp. 245-259.

[19] Eidenbenz, S., Resta, G., Santi, P.: COMMIT: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes. In: Proceedings of 19th IEEE International, Parallel and Distributed Processing Symposium (IPDPS), Denver, Colorado, USA, 3-8 April 2005, pp. 239-249.

[20] Janzadeh, H., Fayazbakhsh, K., Dehghan, M., Fallah, M. S.: A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. Future Generation Computer Systems 25(8), 926-934 (2009).

[21] Mahmoud, M. M. E. A., Shen, X.(S).: A secure payment scheme with low communication and processing overhead for multihop wireless networks. IEEE Transactions on Parallel and Distributed Systems 24(2), 209-224 (2013).

[22] Jakobsson, M., Buttyan, L., Hubaux, J.-P.: A micro-payment scheme encouraging collaboration in multi-hop cellular networks. In: Proceedings of 7th International Financial Cryptography Conference, Gosier, Guadeloupe, 27-30 January 2003, pp. 15-33.

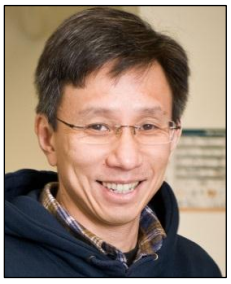
[23] Salem, N. B., Buttyan, L., Hubaux, J.-P., Jakobsson, M.: Node cooperation in hybrid ad hoc networks. IEEE Transactions on Mobile Computing, 5(4), 365-376, 2006.
[24] Mahmoud, M. M. E. A., Shen, X.(S).: An integrated stimulation and punishment mechanism for thwarting packet drop in multihop wireless networks. IEEE Transactions on Vehicular Technology 60(8), 3947-3962 (2011).
[25] Mahmoud, M. M. E. A., Shen, X.(S).: FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for hybrid ad hoc networks. IEEE Transactions on Mobile Computing 11(5), 753-766 (2012).
[26] Weyland, A., Staub, T., Braun, T.: Comparison of motivation-based cooperation mechanisms for hybrid wireless networks. Computer Communications 29(13-14), 2661-2670 (2006).
[27] Marti, S., Giuli, T. J., Lai, K., Baker, M. : Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, USA, 6-11 August 2000, pp. 255-265.
[28] Buchegger, S., Boudec, J.-Y. L. : Performance analysis of the CONFIDANT protocol. In: Proceedings of 3rd ACM International Symposium on Mobile Ad hoc Networking and Computing (MOBIHOC), Lausanne, Switzerland, 9-11 June 2002, pp. 226-236.
[29] Michiardi, P., Molva, R.: CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proceedings of 6th Joint Working Conference on Communications and Multimedia Security, Netherlands, 26-27 September 2002, pp. 107-121.
[30] He, Q., Wu, D., Khosla, P.: SORI: A secure and objective reputation based incentive scheme for ad hoc networks. In: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 21-25 March 2004, pp. 825-830.
[31] Bansal, S., Baker, M.: Observation-based cooperation enforcement in ad hoc networks. In: Technical Report cs.NI/0307012. Computer Science Department, Stanford University, USA, (2003).
[32] Guo, J., Liu, H., Dong, J., Yang, X.: HEAD: A hybrid mechanism to enforce node cooperation in mobile ad hoc networks. Tsinghua Science and Technology 12(1), 202207 (2007).
[33] Hu, J., Burmester, M.: LARS: A locally aware reputation system for mobile ad hoc networks. In: Proceedings of the 44th Annual Southeast Regional Conference, Melbourne, Florida, USA, 10-12 March 2006, pp. 119-123.
[34] Conti, M., Gregori, E., Maselli, G.: Towards reliable forwarding for ad hoc networks. In: Proceedings of Personal Wireless Communications (PWC), Venice, Italy, 23-25 September 2003, pp. 790804.
[35] Dewan, P., Dasgupta, P., Bhattacharya, A.: On using reputations in ad hoc networks to counter malicious nodes. In: Proceedings of the 10th International Conference on Parallel and Distributed Systems (ICPADS), Newport Beach, CA, USA, 7-9 July 2004, pp. 665-672.
[36] Refaei, M.T., Srivastava, V., DaSilva, L., Eltoweissy, M.: A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In: Proceedings of Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous), San Diego, California, USA, 17-21 July 2005, pp. 3-11.
[37] Balakrishnan, K., Deng, J., Varshney, P.K.: TWOACK: Preventing selfishness in mobile ad hoc networks. In: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 13-17 March 2005, pp. 2137-2142.
[38] Liu, K., Deng, J., Varshney, P.K., Balakrishnan, K. : An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing 6(5), 536550 (2007).
[39] Chong, Z.-K., Tan, S.-W., Goi, B.-M., Ng, B.C.-K.: Outwitting smart selfish nodes in wireless mesh networks. International Journal of Communication Systems 26(9), 11631175 (2013).
[40] Buchegger, S., Le Boudec, J-Y.: The effect of rumor spreading in reputation systems for mobile ad-hoc networks. In: Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), INRIA Sophia-Antipolis, France, 3-5 March 2003, pp. 1-10.
[41] Ferraz, L. H. G., Velloso, P. B., Duarte, O. C. M. B.: An accurate and precise malicious node exclusion mechanism for ad hoc networks. Ad Hoc Networks 19, 142-155 (2014).
[42] Eissa, T., Abdul Razak, S., Khokhar, R., Samian, N.: Trust-Based routing mechanism in MANET: design and implementation. Mobile Networks and Applications 18(5), 666-677 (2013).
[43] Yu, M., Zhou, M., Su, W.: A secure routing protocol against byzantine attacks for manets in adversarial environments. IEEE Transactions on Vehicular Technology 58(1), 449-460 (2009).
[44] Zhang, C., Zhu, X., Song, Y., Fang, Y.: A formal study of trust-based routing in wireless ad hoc networks. In: Proceedings of the 29th IEEE International Conference on Information Communications (INFOCOM), San Diego, CA, USA, 15-19 March 2010, pp. 1-9.
[45] Charilas, D.E., Georgilakis, K. D., Panagopoulos, A. D.: ICARUS: hybrId inCentive mechAnism for coopeRation stimUlation in ad hoc networkS. Ad Hoc Networks 10(6), 976-989 (2012).
[46] Jaramillo, J.J., Srikant, R.: DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks. In: Proceedings of the 13th annual ACM international conference on Mobile computing and networking (MobiCom '07), Montreal, Canada, 9-14 September 2007, pp. 87-98.
[47] Shen, H., Li, Z.: ARM: An account-based hierarchical reputation management system for wireless ad hoc networks. In: 28th International Conference on Distributed Computing Systems Workshops (ICDCS '08), Beijing, China, 17-20 June 2008, pp. 370-375.
[48] Wang, X., Cai, Y., Li, Z.: A novel hybrid incentive mechanism for node cooperation in mobile cyber-physical systems. International Journal of Parallel, Emergent and Distributed Systems 29(3), 316-336 (2014).
[49] Milan, F., Jaramillo, J. J., Srikant, R.: Achieving cooperation in multihop wireless networks of selfish nodes. In: Proceedings of Workshop on Game Theory for Communications and Networks (GameNets), Pisa, Italy, 14th October 2006, pp. 1-10.
[50] Ng, S.K., Seah, W. K. G.: Game-theoretic approach for improving cooperation in wireless multihop networks. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 40(3), 559-574 (2010).
[51] Felegyhazi, M., Hubaux, J. P., Buttyan, L.: Nash equilibria of packet forwarding strategies in wireless ad hoc networks. IEEE Transactions on Mobile Computing 5(5), 463-476 (2006).
[52] Niu, B., Zhao, H. V., Hai, J.: A cooperation stimulation strategy in wireless multicast networks. IEEE Transactions on Signal Processing 59(5), 2355-2369 (2011).
[53] Han, Z., Ji, Z., Liu, K. J. R.: A cartel maintenance framework to enforce cooperation in wireless networks with selfish users. IEEE Transactions on Wireless Communications 7(5), 18891899 (2008).

[54] Fudenberg, D., Tirole, J.: Game Theory. MIT Press, Cambridge, MA (1991)
[55] Srivastava, V., Neel, J., Mackenzie, A. B., Menon, R., Dasilva, L. A., Hicks, J. E., Reed, J. H., Gilles, R. P.: Using game theory to analyze wireless ad hoc networks. IEEE Communications Surveys and Tutorials 7(4), 46-56 (2005).
[56] Akkarajitsakul, K., Hossain, E., Niyato, D., Kim, D. I.: Game theoretic approaches for multiple access in wireless networks: A survey. IEEE Communications Surveys and Tutorials 13(3), 372-395 (2011).
[57] MacKenzie, A.B., DaSilva, L.: Game theory for wireless engineers. Morgan and Claypool. (2006).
[58] Charilas, D. E., Panagopoulos, A. D.: A survey on game theory applications in wireless networks. Computer Networks 54(18), 3421-3430 (2010).
[59] Huang, L., Li, L., Liu, L., Zhang, H., Tang, L.: Stimulating cooperation in route discovery of ad hoc networks. In: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks (Q2SWinet '07), Chania, Crete Island, Greece, 22-26 October 2007, pp. 39-46.
[60] Zhang, Z., Shi, J., Chen, H-H., Guizani, M., Qiu, P.: A cooperation strategy based on nash bargaining solution in cooperative relay networks. IEEE Transactions on Vehicular Technology 57(4), 2570-2577 (2008).
[61] Sun, Y., Guo, Y., Ge, Y., Lu, S., Zhou, J., Dutkiewicz, E.: Improving the transmission efficiency by considering non-cooperation in ad hoc networks. The Computer Journal 56(8), 1034-1042 (2013).
[62] Lee, J.-F., Liao, W., Chen, M. C.: An incentive-based fairness mechanism for multi-hop wireless backhaul networks with selfish nodes. IEEE Transactions on Wireless Communications 7(2), 697-704 (2008).
[63] Zhong, S., Wu, F.: A collusion-resistant routing scheme for noncooperative wireless ad hoc networks. IEEE/ACM Transactions on Networking 18(2), 582-595 (2010).
[64] Refaei, M. T., Rong, Y., DaSilva L. A, Choi, H-A.: Detecting node misbehavior in ad hoc networks. In: Proceedings of IEEE International Conference on Communications (ICC), Glasgow, Scotland, 24-28 June 2007, pp. 3425-3430.
[65] Toledo, A. L., Wang, X.: Robust detection of selfish misbehavior in wireless networks. IEEE Journal on Selected Areas in Communications 25(6), 1124-1134 (2007).
[66] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Nov. 1997. P802.11.
[67] Lei, H., Liu, L.: Extended watchdog mechanism for wireless sensor networks. Journal of Information and Computing Science 3(1), 39-48 (2008).
[68] Liang, G., Agarwal, R., Vaidya, N.: When watchdog meets coding. In: Proceedings of the 29th IEEE International Conference on Information Communications (INFOCOM), San Diego, CA, USA, 15-19 March 2010, pp. 2267-2275.
[69] Hernandez-Orallo, E., Serrat, M. D., Cano, J., Calafate, C. T., Manzoni, P.: Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Communications Letters 16(5), 642-645 (2012).
[70] Just, M., Kranakis, E., Wan, T.: Resisting malicious packet dropping in wireless ad hoc networks. In: Proceedings of International Conference on Ad-Hoc, Mobile, and Wireless Networks (ADHOC-NOW), Montreal, Canada, 8-10 October 2003, pp. 151-163.
[71] Awerbuch, B., Holmer, D., Nita-Rotaru, C., Rubens, H.: An on-demand secure routing protocol resilient to byzantine failures. In: Proceedings of the ACM Workshop on Wireless Security (WiSE), Atlanta, GA, USA, 28 Sept. 2002, pp. 21-30.
[72] Wang, B., Soltani, S., Shapiro, J. K., Tan, P.-N.,: Local detection of selfish routing behavior in ad hoc networks. In: Proceedings of 8th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN), Las Vegas, Nevada, USA, 7-9 Dec. 2005, pp. 392-399.
[73] Tseng, C.-Y., Balasubramanyam, P., Ko, C., Limprasittiporn, R., Rowe, J., Levitt, K.: A specification-based intrusion detection system for AODV. In: Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 27-30 Oct. 2003, pp. 125-134.
[74] Ye, X., Li, J.: An FSM-based automatic detection in AODV for ad hoc network. In: Proceedings of International Symposium on Computer Network and Multimedia Technology (CNMT), Wuhan, China, 18-20 Dec. 2009, pp. 1-5.
[75] Orset, J.-M., Alcalde, B., Cavalli, A.: An EFSM-based intrusion detection system for ad hoc networks. In: Proceedings of the 3rd Automated Technology for Verification and Analysis (ATVA), Taipei, Taiwan, 4-7 Oct. 2005, pp. 400-413.
[76] Lin, H.-C., Sun, M.-K., Huang, H.-W., Tseng, C.-Y.H., Lin, H.-T.: A specification-based intrusion detection model for wireless ad hoc networks In: Proceedings of the 3rd International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA), Kaohsiung City, Taiwan, 26-28 Sept. 2012, pp. 252-257.
[77] Sorin, S.: On repeated games with complete information. Mathematics of Operations Research 11(1), 147-160 (1986).
[78] Mailath, G.J., Obara, I., Sekiguchi, T.: The maximum efficient equilibrium payoff in the repeated prisoners dilemma. Games and Economic Behavior 40(1), 99-122 (2002).
[79] Mailath, G.J., Matthews, S. A., Sekiguchi, T.: Private strategies in finitely repeated games with imperfect public monitoring. Contributions to Theoretical Economics 2(1), 1-2 (2002).
[80] Kandori, M.: Randomization, communication, and efficiency in repeated games with imperfect public monitoring. Econometrica 71(1), 345-353 (2003).
[81] Green, E.J., Porter, R. H.: Noncooperative collusion under imperfect price competition. Econometrica 52(1), 87-100 (1984).
[82] Srivastava, V., Dasilva, L. A.: Equilibria for node participation in ad hoc networks - an imperfect monitoring approach. In: Proceedings of IEEE International Conference on Communications (ICC), Istanbul, Turkey, 11-15 June 2006, pp. 3850-3855.
[83] Bhaskar, V., Eric, V. D. : Moral hazard and private monitoring. Journal of Economic Theory 102(1), 16-39 (2002).
[84] Compte, O.: On failing to cooperate when monitoring is private. Journal of Economic Theory 102(1), 151-188 (2002).
[85] Kandori, M.: Introduction to repeated games with private monitoring. Journal of Economic Theory 102(1), 1-15 (2002).
[86] Aoyagi, M.: Collusion in dynamic bertrand oligopoly with correlated private signals and communication. Journal of Economic Theory 102(1), 229248 (2002).
[87] Compte, O.: Communication in repeated games with imperfect private monitoring. Econometrica 66(3), 597626 (1998).
[88] Kandori, M., Matsushima, H.: Private observation, communication and collusion. Econometrica 66(3), 627652 (1998).
[89] Rebahi, Y., Mujica-V, V. E., Sisalem, D.: A reputation-based trust mechanism for ad hoc networks. In: Proceedings of the 10th IEEE

Symposium on Computers and Communications (ISCC), Cartagena, Spain, 27-30 June, 2005, pp 37-42.
[90] Samian, N., Seah, W. K. G., Chen, G.: Quantifying selfishness and fairness in wireless multihop networks. In: Proceedings of 38th Annual IEEE Conference on Local Computer Networks (LCN), Sydney, Australia, 21-24 Oct. 2013, pp. 270-278.

Normalia Samian is a tutor at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). She obtained her Diploma (Engineering), B.Sc (Computer Science) from UPM where she received Best UPM Student Award in 2006. In 2010, she received her M.Sc (Computer Science) from Universiti Teknologi Malaysia (UTM) in the area of Wireless Networks Security and was nominated for Best Academic Award candidate. Currently, she's pursuing her Ph.D degree in UPM in the area of cooperation in wireless multihop networks. Her research interests include ad hoc networks security, trust management in MANETs and game theoretical approaches for wireless multihop networks.

Zuriati Ahmad Zukarnain is an Associate Professor at the Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM) Malaysia. She is the head for High Performance Computing Section at Institute for Mathematics and Research (INSPEM), University Putra Malaysia. She received her PhD from the University of Bradford, UK. Her research interests include: Efficient multiparty QKD protocol for classical network and cloud, load balancing in the wireless ad hoc network, quantum processor unit for quantum computer, Authentication Time of IEEE 802.15.4 with Multiple-key Protocol, Intra-domain Mobility Handling Scheme for Wireless Networks, Efficiency and Fairness for new AIMD Algorithms and a Kernel model to improve the computation speedup and workload performance. She has been actively involved as a member of the editorial board for some international peer-reviewed and cited journals. Dr. Zuriati is currently undertaking some national funded projects on QKD protocol for cloud environment as well as routing and load balancing in the wireless ad hoc networks.



Winston K. G. Seah received the Dr.Eng. degree from Kyoto University, Kyoto, Japan, in 1997. He is currently Professor of Network Engineering in the School of Engineering and Computer Science, Victoria University of Wellington, New Zealand. Prior to this, he has worked for more than 16 years in mission-oriented research, taking ideas from theory to prototypes, most recently, as a Senior Scientist (Networking Protocols) in the Institute for Infocomm Research (I2R), Singapore. He is actively involved in research in the areas of mobile ad hoc and sensor networks, and co-developed one of the first Quality of Service (QoS) models for mobile ad hoc networks. His latest research interests include wireless sensor networks powered by ambient energy harvesting (WSN-HEAP), wireless multi-hop networks, software defined networking, and mobility-enhanced protocols and algorithms for networked swarm robotics and sensing applications in terrestrial and oceanographic networks. He is a Senior Member of the IEEE. Homepage: http://www.ecs.vuw.ac.nz/ winston/.

Azizol Abdullah obtained his Master of Science in Engineering (Telematics) from the University of Sheffield, UK in 1996 and his PhD in Distributed System from Universiti Putra Malaysia, Malaysia in 2010. He is a Senior Lecturer at Department Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia and currently hold the position of Deputy Dean of Academics and Student Affairs. His main research areas include cloud and grid computing, network security, wireless and mobile computing and computer networks.

Zurina Mohd Hanapi received her first degree in BSc. Computer and Electronic System from the University of Strathclyde, Glasgow, UK in 1999. The author then received her master degree in MSc. Computer and Communication System Engineering from Universiti Putra Malaysia (UPM), Selangor, Malaysia in 2004 and Ph.D from the Universiti Kebangsaan Malaysia (UKM) in 2011. Currently she is a senior lecturer in the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, UPM. She had published more than 20 papers in the cited journals and conferences in the area of security and wireless sensor network. Her current research interests are on security, routing, wireless sensor network, wireless network, distributed computing, and cyber-physical-system. Dr. Zurina is a member on Malaysian Security Committee Research (MSCR) and IEEE.