A STUDY ON COOPERATION ENFORCEMENT BETWEEN NODES IN MOBILE AD HOC NETWORKS

[1]NOR EFFENDY OTHMAN, [2]STEFAN WEBER, [3]ROSILAH HASSAN

[1, 3]Network and Communication Technology Lab, Software Technology and Management Research Centre,
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia.
[1, 2]Distributed Systems Group, School of Computer Science and Statistics, Trinity College Dublin, Ireland.
E-mail: [1]effendy@ftsm.ukm.my

ABSTRACT

Traditional infrastructure-based networks are formed around an infrastructure of static, dedicated components that connect the individual end points such as desktop computers and servers. The exponential rise in the number of wireless communication devices will render the provision of infrastructure-based solutions infeasible and researchers have been investigating the provision of alternative communication structures in the form of mobile ad hoc networks (MANETs). A MANET is a collection of low-resourced mobile nodes that communicate over wireless links without the need of fixed infrastructure. The network operates in distributed fashion, where all networking functions including route discovery and packet delivery are executed by the nodes themselves. Nodes in a MANET rely on multi-hop communication to communicate with nodes outside their transmission ranges. However, this can only be realized if all these nodes are willing to cooperate with each other i.e. are not reluctant to forward others' packets. In self-organized MANETs such as civilian MANETs, each node acts as its own authority and may not share common goals with other nodes. Moreover, nodes in such networks are self-interested and tempted to drop others' packets to preserve of their own limited resources e.g. battery power and computational capability. Such selfishness and non-cooperative behavior can make it impossible to achieve multi-hop communication and have a negative effect on the overall network performance. A large number of studies have proposed different cooperation enforcement mechanisms for MANETs. In this review paper, we discuss the rationale of cooperation enforcement in MANETs and the characteristics of a cooperation enforcement model. We also review different types of existing approaches to cooperation enforcement in MANETs and analyze them in order to provide justification for moving towards tag-based approach in enforcing cooperation between nodes in MANETs. Then we introduce the concepts found in tag-based cooperation and review existing tag-based approaches.

Keywords: *MANET, Cooperation, Selfish Nodes, Packets Forwarding, Tag-based Cooperation*

1. INTRODUCTION

A mobile ad hoc network is formed by a set of mobile nodes that communicate over wireless links without the necessity of pre-existing infrastructure. The network operates in a distributed fashion, where all networking functions including route discovery and packet delivery must be performed by the nodes themselves. Nodes in a mobile ad hoc network rely on multi-hop communication to communicate with nodes that are out of their transmission ranges. For instance, if a destination node is out of a source node's direct transmission range, nodes between them are expected to serve as routers, forwarding packets from the source to the destination [1]. Thus, cooperation between nodes is necessary to establish an operational network.

Mobile ad hoc networks (MANETs) possess a number of unique characteristics which create challenges for the network. One of the characteristics is the lack of fixed infrastructure. MANETs are self-organized; there is no central authority that perform administrative and management functionalities. Instead, all networking functions including route discovery and packet delivery are executed by the nodes themselves, in a decentralized fashion. In addition, the dynamic mobility of nodes in mobile ad hoc networks, in other words, nodes freely join and leave the network frequently results in frequently changing topology, decreasing the stability of the links and routes [2]. The mobility of nodes also indicates that most of the time nodes are not placed in protected spaces such as locked rooms. Thus, they are easily stolen or compromised. Furthermore, communication in MANETs, as in other wireless networks, takes place over a wireless channel. Such communication suffers from errors such as fading and interference. Finally, distant nodes depend on multi-hop forwarding to communicate with each other as they have limited transmission ranges. This requires nodes in the network to be highly cooperative on forwarding packets for each other. However, mobile nodes generally have limited resources e.g. battery power, processing capacity and bandwidth. They tend to be selfish in order to preserve their resources.

1.1 Selfish Misbehavior

Selfish misbehavior refers to the act of reluctant to spend one's own resources for the benefit of others. In MANETs, a typical selfish misbehavior may include nodes that refuse to spend their resources such as battery power, processing capacity and/or bandwidth to forward packets for others but expect others to forward packets for them [3].

Michiardi and Molva [4] introduce three categories of selfish nodes. The first category of selfish nodes refuse to contribute to the data packet forwarding but they participate in the network routing and maintenance. Selfish nodes in the second category refuse to participate in the route discovery and maintenance, thereby their forwarding function are turned off for all packets. In the third category, selfish nodes behave according to their energy level. They function normally if their energy level is higher than a specified high threshold. When the level drops to between the high and low threshold, they behave as same as the selfish nodes in the first category. Finally, if their energy level drops lower than the low threshold, they will behave as the selfish nodes in the second category.

Buttyan and Hubaux [5] show that when there is an average of 5 hops between the source and destination, around 80% of the transmission energy will be spent on packet forwarding. Hence, in self-organized MANETs where nodes are battery-powered, it is rational for the nodes to be selfish in order to conserve their limited energy. The selfish misbehavior, although rational for individual nodes, can be a significant threat to MANETs performance [3, 4, 5]. It can cause problems such as throughput degradation, increasing latency and network partition. For example, Marti et al. [3] show by simulation that if 10 to 40% of the nodes in the network do not contribute to packet forwarding, then the average throughput would decrease by 16 to 32%. Furthermore, Buttyan and Hubaux [6] show that the misbehavior will cause a higher throughput degradation rate in larger networks.

2. COOPERATION ENFORCEMENT RATIONALE

There are two rationales for cooperation enforcement in MANETs. The first one is to correlate between a node's contribution to the network i.e. forwarding packets and the service it received from the network (i.e. having its own packets forwarded by other nodes). The correlation is that the higher the contribution of a node to the network, the higher its chance to receive service from the network. If there is no correlation between the two, packets forwarding will be unattractive to nodes. Consequently, each node in the network will maximize its utility by not contributing to packet forwarding. If all nodes follow this behavior, then the performance of the network will significantly decrease (refer section (1.1)).

Secondly, as there is no central authority in self-organized MANETs, cooperation enforcement serves as a mechanism to defend against selfish misbehavior in the networks. The main idea of the existing approaches is to provide incentives for nodes to forward packets not of direct interest to themselves. Cooperative nodes should be rewarded while selfish nodes should be punished. Different cooperation enforcement systems have been proposed to provide incentive for selfish nodes to cooperate. In the existing approaches, two types of incentive are used i.e. credit and reputation. Besides that, the application of game-theory in cooperation enforcement systems has also been investigated. Figure 1 illustrates the overview of the existing cooperation enforcement approaches.

3. CHARACTERISTICS OF COOPERATION ENFORCEMENT MODELS FOR MANETS

This section lists the characteristics of cooperation enforcement model targeting MANETs. These characteristics can be divided into generic characteristics and characteristics that are specific to certain types of cooperation enforcement models.

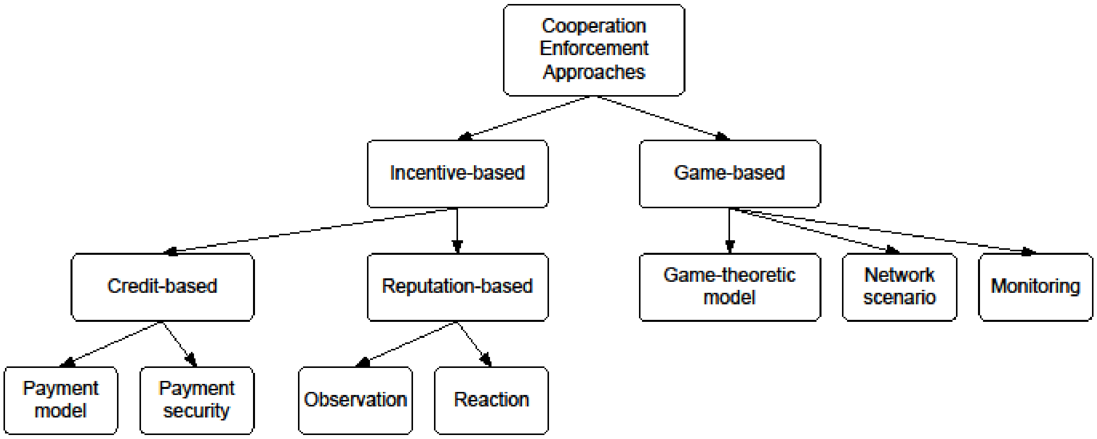

Figure 1: Overview Of Existing Cooperation Enforcement Approaches

3.1 Cooperation Enforcement Model Generic Characteristics

Cooperation enforcement model generic characteristics include whether the enforcement is managed by centralized or distributed entity, execution of the enforcement and types of enforcement.

3.1.1 Management

In self-organizing MANETs that might involve a large number of nodes, centralized management of cooperation enforcement might not scale well. This domain needs decentralized cooperation enforcement approaches. In decentralized cooperation enforcement, every nodes play a part in deciding, what enforcement actions to execute and how to execute them. This requires additional algorithms and techniques, such as monitoring, to enable the nodes to detect when and how to enforce cooperation.

3.1.2 Execution

The execution of cooperation enforcement in MANETs can be proactive or reactive. For proactive execution, the enforcement mechanism is designed so that the emergence of selfish nodes is prevented. Proactive execution is normally found in credit-based models whereby a node has to earn sufficient credits through forwarding other nodes' packets before it could send its own packets. Reactive execution, on the other hand, is normally found in reputation-based models and does not prevent selfish nodes from emerging in the network. Hence, mechanisms to detect and punish the selfish nodes are needed.

3.1.3 Types

Cooperation enforcement models can be classified according to how the models enforce cooperation between nodes in the network. Existing models can be classified into incentive-based and game-based models. The incentive-based models can be further classified as credit-based and reputation based models.

3.2 Credit-based Model Characteristics

In credit-based models [5, 7, 8, 9, 10], the nodes receive credits as an incentive for forwarding packets for others. These credits can then be used to pay other nodes for forwarding their packets. Selfish nodes, which always refuse to forward other nodes' packets, cannot earn any credits. Thus, they are prevented from using the network. Existing models operate based on payment models that regulate the dealing between nodes for packet forwarding. They also require protection modules to prevent payment fraud.

3.2.1 Payment model

Most payment models proposed in the literature are based on payment per packet. Buttyan and Hubaux [8] proposed two payment models called packet purse model (PPM) and packet trade model (PTM). PPM requires the source node to pay intermediate nodes for packet forwarding. The source loads virtual credits into packets and intermediate nodes receive the credits as a reward for their packet forwarding service. Packets with insufficient credits will be ignored by intermediate nodes. On the other hand, PTM requires the destination node to take the responsibility of paying intermediate nodes. During the packet forwarding process, each intermediate node buys the packet from previous node and sells it to the next node at a higher price. As a result, the destination node pays the final price.

3.2.2 Payment security

The existence of currency in the systems requires some kind of security module to prevent fraud. The module should be able to prevent nodes from exploiting the credits in the system to their favor. Virtual currency counter [5] and centralized third-party service [9, 10] have been proposed to prevent payment fraud.

3.3 Reputation-based Model Characteristics

In reputation-based models [3, 11, 12, 13], each node observes the behavior of others in packet forwarding to assess their reputations and stores this information locally to distinguish between selfish and cooperative nodes in future interactions. When a selfish node is identified, it distributes the information to other nodes in the network so that the selfish node can be avoided and/or punished. Existing reputation-based models typically consist of two main stages i.e. Observation and reaction to selfish behavior.

3.3.1 Observation

During the observation stage, a node has to monitor the transmission of its neighboring nodes to determine if they are forwarding packets correctly or not. It is assumed that nodes could overhear their neighbor's transmission promiscuously [3, 11, 13]. Consider a multi-hop scenario where node *S* sends a packet to node *D* through its neighbor, node *A*. All of node *A*'s neighbors including node *S* are able to observe node *A*'s transmission by overhearing. They can observe whether node *A* receives the packet from node *S* and forwards it to node *D* or not. If node *A* receives the packet but does not forward it, its neighboring nodes observe this as a packet dropping activity which is considered as selfish behavior. As a consequence, node *A* will have a bad reputation. Otherwise, node *A* is seen as a cooperative node which gives it a good reputation.

Observation collected by the nodes can be classified into first-hand and second-hand observation. The former is a node's direct observation of its neighboring nodes while the latter is provided by other nodes in a node's neighborhood. Most existing reputation-based systems utilize both types of observations. They can be further categorized based on how they handle the second-hand observation. The first category refers to approaches that accept second-hand observation without any evaluation of trustworthiness. The second category, on the other hand, refers to approaches that evaluate the trustworthiness of second-hand observation.

3.3.2 Reaction to selfish nodes

Based on the observation, a node then decides on how it should react to the environment. In the literature, two types of reaction to selfish nodes can be identified i.e. avoidance [3] and isolation [11, 12]. In avoidance reaction, selfish nodes are avoided during packet forwarding but they are not blocked from sending their own packets, while in isolation reaction, selfish nodes are avoided and blocked from sending their own packets.

3.4 Game-based Model Characteristics

Besides the incentive-based models, game theory has been applied by researchers to mathematically analyze the cooperation problem at the network layer i.e. participation in routing and forwarding in ad hoc networks. Game theory is a collection of models which can be used to study the interaction between decision-makers [14]. In game theory, the interaction is modeled as a game in which the decision-makers act as players. The goal is to find a solution of the game i.e. the outcomes that may emerge in the game.

Several researchers have proposed game-theoretic models for packet forwarding operation [15, 16, 17, 18]. They considered different network scenarios in defining the models and analyzed the models to find an equilibrium point of cooperation strategies.

3.4.1 Game-theoretic models

Game-theoretic models can be classified into non-cooperative games and cooperative games. Most of the work presented in the literature modeled the packet forwarding operation as a non-cooperative game. In a non-cooperative game, each player is assumed to act independently, without any form of coalitions [19]. This aspect of the game is similar to the self-organized mobile ad hoc network environment in which players i.e. the nodes belong to different authority and they can choose to forward or drop packets independently.

The players, whether in cooperative or non-cooperative games, are also assumed to be rational in the sense they always choose strategies that maximize their own payoffs. Selfish nodes in MANETs can be considered as rational players in which they always try to maximize their energy for their own use. In the existing work, assuming all players are rational, they try to find a Nash equilibrium of packet forwarding strategies from the non-cooperative game. A Nash equilibrium is a state where no player can increase its payoff any higher than the current payoff by deviating from its strategy while other players keep their strategies unchanged. Therefore, a set of strategies in a Nash equilibrium can satisfy all players.

In the literature, game-theoretic models have been developed to study the cooperation of nodes in a wireless ad hoc network with heterogeneous devices [16] and a self-organized mobile ad hoc network [18], as well as to identify the conditions that allow cooperation to exist in a static ad hoc network [15].

3.4.2 Network scenarios

Although these game-based approaches share the common goal of finding a Nash equilibrium for the game, they analyzed their models based on different network scenarios i.e. random connection between source and relay nodes [16], static ad hoc network [15] and noisy network with malicious nodes [18].

3.4.3 Monitoring

Monitoring is a key component in game-based approaches as each node needs to gather some inputs from the environment in order to determine the best strategy to play. It can be classified into per-session monitoring [15, 16, 17] and per-node monitoring [18].

Per-session monitoring requires each node to monitor packets forwarding by other nodes within a given time slot, assuming that a node sends more than one packet and the route remains unchanged in each time slot. Therefore, each node does not need to maintain records for every node it encounters in the network. Instead, it maintains only records of its experience per session. This is an advantage that per-session monitoring has over per-node monitoring as it reduces the storage capacity requirement of each node. A common characteristic of the approaches that use per-session monitoring is that each node tracks only the normalized throughput it has experienced in each session. This also helps in reducing the amount of data that needs to be stored at each node.

Per-node monitoring, on the other hand, requires each node to monitor the behavior of every node it interacts with in the network and maintains records of those nodes.

4. REVIEW OF EXISTING COOPERATION ENFORCEMENT MODELS

The reviews focus on the degree to which the existing models represent the characteristics of a cooperation enforcement model. The literature available on cooperation enforcement models is vast; however, we try to cover a sample of representative approaches.

4.1 Credit-based Models

A general overview of credit-based cooperation enforcement models was provided in section (3.2). This section discusses existing credit-based models with respect to the characteristics described in section (3.2).

4.1.1 Nuglets

Buttyan and Hubaux proposed a virtual currency called nuglets [6] in their approach using decentralized management and proactive execution. Their approach operates using either PPM or PTM payment model discussed in section (195.2.1). If it operates using PPM, the source node has to estimate the amount of nuglets required to send its packets to the destination node as packets with insufficient packets will be discarded by intermediate nodes. On the other hand, if it operates using PTM, the destination node pays the final price of the packets. Buttyan and Hubaux later improved their approach by using nuglets counter [5]. The nuglets counter, however, needs to be implemented in tamper-resistant hardware module in order to provide security and avoid modification of the counter.

4.1.2 Sprite

Zhong et al. proposed a model named Sprite [10] which operates based on centralized management and proactive execution. Sprite works based on PPM payment model except that for payment security, they propose a central server which provides credit clearance service for nodes. In Sprite, whenever a node receives a packet that needs to be forwarded, it keeps a receipt as a record of previous node's contribution in forwarding the packet. This process repeats for each packet sent and until the packet reaches the destination node. The receipts are then reported to CCS whenever the nodes have connection to CCS. After receiving all the receipts, CCS rewards the intermediate nodes involved in the packets forwarding and charges the source node accordingly.

4.1.3 PIFA

Protocol Independent Fairness Algorithm (PIFA) [9] has centralized management and proactive execution. Its payment model is similar to Sprite where it also uses centralized server to manage the credits of nodes in the network and prevent payment fraud. The server is known as credit manager. However, PIFA is different than Sprite in the way that nodes report to credit manager. In PIFA, each node periodically sends a report containing the number of packets it forwarded in a specified time interval. Credit manager then compares all received reports to determine their credibility and rewards each node accordingly.

4.1.4 Ad hoc-VCG

Similar to nuglets, Ad hoc-VCG [7] has decentralized management and proactive execution. It also applies the PPM payment model but with improvement in determining the cost to send packets from source to destination node. For Ad hoc-VCG, Anderegg and Eidenbenz suggested a two-phase payment model. During the first phase which is the route discovery, a destination node calculates the amount of payment for intermediate nodes based on the received route request messages and then notifies the source node. In the second phase i.e. packets forwarding phase, the source node pays intermediate nodes based on the notified amount. They however did not focus on payment security.

4.2 Reputation-based Models

A general overview of reputation-based cooperation enforcement models was provided in section (3.3). This section discusses existing reputation-based models with respect to the characteristics described in section (3.3).

4.2.1 Watchdog and pathrater

Watchdog and pathrater approach [3] employs decentralized management and reactive execution. In this approach, each node has a watchdog and a pathrater. The watchdog is responsible for overhearing neighboring nodes' transmission in order to observe their packet forwarding activities. It overhears promiscuously in which it can observe all packets that are transmitted within a node's coverage. If an observing node detects a neighbor node has dropped packets more than a predefined threshold, it sends a notification to the source node of the packets. The pathrater component of the source node then uses the received information to calculate rating for the misbehaving node. Pathrater maintains a table of other nodes' ratings and uses the information to determine best routes for sending packets in order to avoid misbehaving nodes.

In terms of observation characteristic, watchdog and pathrater is one of the approaches that accept second-hand observation without any evaluation of trustworthiness. In this approach, second-hand observation is sent to the source node whenever the watchdog of its neighbor detects misbehavior by nodes that are out of the source node's neighborhood. The pathrater of the source node then use the observation to update its rating list. Each node, through its pathrater, keeps a rating for every other node it encounters in the network.

The watchdog and pathrater system deploys avoidance reaction when selfish nodes are detected in the network. Other than maintaining ratings for other nodes, the pathrater component is also responsible for calculating a path reliability by averaging the ratings of nodes in the path. A selfish node, which has a low rating, will cause a path to be less reliable. As a result, other path with the highest reliability is selected for sending packets. Thus, the selfish node is avoided. However, it is still allowed to transmit its own data whenever it wants.

4.2.2 CONFIDANT

CONFIDANT [11] has decentralized management and reactive execution. It consists of four components; known as monitor, trust manager, reputation system and path manager, which are executed in each node. The monitor is an improved version of the watchdog component. In addition to promiscuous listening mode, it also observes how route requests are handled by neighboring nodes. If it detects a misbehaving node, the trust manager sends ALARM messages to neighboring nodes.

In contrast to watchdog and pathrater, CONFIDANT evaluates the trustworthiness of second-hand observation. In this approach, a node records first-hand and trusted second-hand observations of other nodes' routing and forwarding behavior to detect misbehaving nodes. When a neighboring node receives an ALARM message which is a second-hand observation, its trust manager calculates the message trustworthiness based on the trust level of the sender. If the message is considered trustworthy, its reputation system updates the rating of the misbehaving node accordingly. As a consequence, CONFIDANT not only allows the exchange of positive reports between nodes but it also allows nodes to exchange negative reports.

CONFIDANT reacts by isolating selfish nodes. In this approach, besides a local rating list, the reputation system also maintains a black list which contains information of nodes that should be avoided. Similar to the pathrater, the path manager component in CONFIDANT manages the paths ranking. It sorts the paths ranking according to the reputation of nodes in each path. The paths that contain selfish nodes are deleted from the record. Moreover, route requests from blacklisted nodes are not forwarded. This means that the selfish nodes is not just avoided but also punished for their misbehavior. Hence, they are isolated from the network.

4.2.3 CORE

CORE [12] operates based on decentralized management and reactive execution. It consists of two components i.e. a watchdog and a reputation table. The watchdog component is similar to the watchdog discussed in section (4.2.1). In CORE approach, each node classifies its observation of a node into three types of reputation:

- Subjective reputation, which is locally calculated based on first-hand observation.
- Functional reputation, which is related to a specific task or function and given a weight based on its importance. For instance, if data packets forwarding has higher priority than route requests forwarding, then greater weight is given to data packets forwarding when calculating reputation.
- Indirect reputation, which is a reputation value reported based on second-hand observation.

Similar to watchdog and pathrater, CORE does not evaluate the trustworthiness of second-hand observation. However, CORE improves the approach by allowing only positive reports to be spread as indirect reputation. They argue that this method could prevent false broadcasting of negative ratings by malicious nodes. Hence, the second-hand observation can be trusted without being evaluated.

The isolation of nodes in CORE depends on their individual reputation values. Each node calculates a reputation value for every observed node by integrating the observed node's subjective, functional and indirect reputation values. These values are maintained in the reputation table. If a node's reputation is lower than a predefined threshold value, it is isolated from networking. However, the isolated node is allowed to rejoin the network if it cooperates in packet forwarding long enough to increase its reputation above the threshold value.

4.3 Game-based Models

A general overview of game-based cooperation enforcement models was provided in section (3.4). This section discusses existing game-based models with respect to the characteristics described in section (3.4).

4.3.1 Srinivasan et al.

Srinivasan et al. analyzed an ad-hoc network in which the source and relay nodes are chosen randomly [16]. In other words, they did not take into account the network topology. They proposed multi-hop Generous-Tit-For-Tat (m-GTFT) relay acceptance strategy, which has decentralized management and proactive execution, to balance between the energy spent by a node for forwarding other nodes' packets and the energy spent by others in order to forward its packets. They considered a network of heterogeneous devices which include personal digital assistants, laptops and cell phones. Each class of devices has different energy constraints or classes. In the approach, each node maintains four variables for each session type:

- The total of its own requests relayed by others, TRR_{own}.
- The total requests generated by itself, TRG_{own}.
- The total of others' requests relayed by itself, TRR_{others}.
- The total requests it received, TRG_{others}.

Each session type represents each energy class of nodes in the network. Based on the variables, each node calculates two ratios:

$$Ratio_1 = \frac{TRR_{own}}{TRG_{own}} \quad (1)$$

$$Ratio_2 = \frac{TRR_{others}}{TRG_{others}} \quad (2)$$

A node decides to relay or forward a request if

$$Ratio_2 < Ratio_1 + \varepsilon \quad (3)$$

where ε is a positive real number, and $Ratio_2$ does not exceed the maximum relay ratio for the session type.

If the two conditions are not satisfied, then the node rejects or drops the request. They showed that all nodes using m-GTFT relay acceptance strategy form a Nash equilibrium. It is also shown that if a node deviates from the strategy, it will not achieve a throughput rate higher than the optimal value.

They proposed per-session monitoring in their approach which, as mentioned in section (3.4.3), reduces the storage capacity requirement of each node. For example, each node employing the GTFT algorithm only needs to store four variables for each session type or energy class. Hence, the total number of variables stored in each node is bounded by the number of energy classes, independent of the number of nodes, in the network.

4.3.2 Felegyhazi et al.

In relation to Srinivasan et al. work [16], Felegyhazi et al., however, argued that the random participation of source and relay nodes creates a balanced interaction pattern which is the reason unforced cooperation can emerge [15]. To prove this, they analyzed a static ad-hoc network, taking into account the network topology. Their analysis resulted in two noteworthy observations; first, unforced cooperation exists only if the total amount of others' packets forwarded by each node is as same as the total amount of its packets forwarded by others i.e. balanced interaction pattern and second, this condition does not hold i.e. imbalanced interaction pattern exists. Thus, they emphasized the necessity of incentive mechanisms to correct the imbalance.

They concluded that a Nash equilibrium of cooperative strategies can be achieved only if every node forwards the same amount of packets for each other.

4.3.3 Yu and Liu

Yu and Liu, on the other hand, considered a network scenario with malicious nodes and selfish nodes as well as a noisy environment (e.g., packets dropped due to channel errors or link breakage) [18]. In order to find a Nash equilibrium point, they modeled and analyzed a secure routing and packet forwarding game. In the game, each node is either selfish or malicious. For each node, forwarding a packet for other node will incur a cost and having its packet forwarded by other node will give it a gain. The expended energy, for example, can be the cost and application-level metric such as the total size of files sent can be measured as gain. The game involves three stages where in each stage, a node chooses a strategy:

- Route participation, that is where it decide to accept or refuse route requests from other nodes.
- Route selection, that is where it choose one of discovered routes.
- Packet forwarding, that is where it decides to forward or drop other node's packet.

Assuming each node is rational; it chooses strategies that maximize its utility. From their analysis, they found that there exists at least a point of Nash equilibrium. This led them to propose a cooperation strategy that is secure from malicious nodes as well as stimulating cooperation between selfish nodes, for the three stages:

- In route participation, a node accepts a route request only if the source node is not malicious and it has not forwarded the source node's packets more than it has to.
- In route selection, a node chooses the shortest path only if it does not involve any malicious nodes and the expected cost is lower than the expected gain. The calculation of expected gain must consider channel error ratio and hop length.
- In packet forwarding, a node selects whether to forward or drop packets from other node based on the number of its own packets that the other node has attempted to forward.

They showed that a Nash equilibrium is achieved in their model when all nodes use their proposed cooperation strategy in route participation, route selection and packet forwarding stages.

Yu and Liu proposed per-node monitoring in their approach. Although each node only maintains four variables for every node it has communicated with, the total number of variables it stored is bounded by the number of nodes in the network. However, they argued that the per-node monitoring is necessary in a hostile environment so that any malicious node can be detected and punished.

5. ANALYSIS OF COOPERATION ENFORCEMENT MODELS

This section provides an analysis of these existing models focusing on their drawbacks.

5.1 Analysis of Credit-based Models

The credit-based models, as shown in the literature, can be effective in enforcing cooperation between nodes. A selfish node will have no choice but to participate in packet forwarding in order to earn credits for its own packet transmission. However, there are several issues that may arise from the design and implementation of such systems.

First, the requirement of a security module such as tamper-proof hardware in the case of nuglets counter may be difficult to be accepted as it is not always available in a mobile device. Moreover, the existence of third-party service, although it can eradicate the necessity of tamper-proof hardware, contradicts with the MANETs nature of lacking central authority. However, without a security module, a credit-based system could not be guaranteed to be safe and secure.

Second, the existing credit-based models could not prevent selfish behavior from appearing in the network after cooperation has been achieved. For example, a selfish node might try to accumulate credits only as much as it needs to send its own packets. When it gets enough credits, it may decide not to cooperate anymore and drop other nodes' packets. Furthermore, when most intermediate nodes have enough credits for their own use, then there may be no cooperation at all.

Third, a common drawback suffered by credit-based models is they do not consider nodes that are located on the outskirts of a network [20]. Those nodes will not have as many opportunities to relay other nodes' packets as central nodes i.e. nodes located at the physical centre of the network have. Thus, they will earn significantly less than central nodes and might not have enough credits to send their own packets.

Fourth, some of the existing approaches may have a scalability issue. The Sprite approach [10], for example, requires each node to keep a receipt for each message it forwards and to upload all of its receipts to a central credit clearance service for payment claim. In a large network where there is a high rate of multi-hop communication, this approach may incur an increase in overhead in terms of memory size required by the nodes to store their receipts.

These issues must be addressed before credit-based systems can be realized in MANETs.

5.2 Analysis of Reputation-based Models

The reputation-based models may be as effective in encouraging cooperation between nodes as the credit-based systems. Furthermore, the reputation-based models do not require any tamper-proof hardware which is a significant advantage over the credit-based systems. However, they have a few drawbacks that may undermine their performance.

First, the major drawback of reputation-based models lies in the reputation records. Each reputation record stored in a node is linked to a unique identity. Thus, reputation-based models require each node's identity to be persistent to keep the reputations information valid in future interactions. In MANETs where there is no central authority, it is not impossible for a node with a bad reputation to change its identity to avoid punishment unless a reliable authentication scheme is implemented. This is also known as Sybil attack [21].

Second, when a packet is dropped, a node may not know how to differentiate whether it is caused by selfish behavior or some unintentional error such as packet collision. This can lead to false detection of selfish nodes. A high false detection rate would cause many supposedly cooperative nodes to be treated as selfish nodes, which in turn decreases the overall network throughput.

Third, most of the existing approaches are vulnerable to collusion between malicious nodes. Thus, the trustworthiness of distributed second-hand observation could not be guaranteed [22]. For example, in the CORE system, a small group of nodes could collude to distribute positive reports about each other to their neighborhood so that they can build up a good reputation before behaving maliciously for a period.

Fourth, some of the existing approaches may have issues that are specific to their system. As an example, the watchdog and pathrater system does not punish the selfish nodes but instead relieves them from the burden of forwarding. Thus, there is no reason for the nodes to be cooperative.

These drawbacks must first be solved before we can have a reliable reputation-based system for MANETs.

5.3 Analysis of Game-based Models

Although the game-based approaches can lead a network to achieve cooperative equilibrium whereby all nodes in the network are playing optimal packet forwarding strategies, they still have some weaknesses that need to be addressed.

First, as game-based approaches require a monitoring mechanism, they face similar problems as reputation-based approaches. In the per-node monitoring mechanism, each node has a unique identity, which leads to the identity problem discussed in the analysis of reputation-based approaches. Furthermore, they assume perfect monitoring. For example, a node using the per-session monitoring always knows the number of packets transferred in a session while in the per-node monitoring, a node always knows which nodes have dropped its packets. However, perfect monitoring is not always available [18]. A node may have the wrong information as a result of imperfect monitoring. It is not known whether their approaches could stimulate cooperation using an imperfect monitoring mechanism.

Second, each node must have sufficient information about the network, sometimes including private information of other nodes, to determine an optimal strategy for itself. For example, each node in the m-GTFT approach [16] has to know the energy limit for each class and also the number of nodes in each of the class. In a large network, this may be difficult to achieve. The attack-resistant and cheat-proof cooperation stimulation approach [18], on the other hand, does not require nodes to know about the information. However, each node has to maintain sufficient information of every other node that interacted with it. This may require large storage overhead as the amount of information that needs to be maintained is bounded by the number of nodes in the network.

5.4 Summary of Analysis

Table 1 compares the management, features and issues of the existing cooperation enforcement approaches.

In general, a scalable and distributed credit-based system can be achieved only if it implements tamper-proof hardware. Without tamper-proof hardware, the system has to implement a central credit server which limits the scalability of the system. In the reviewed credit-based approaches, the problem of excessive credits, which is discussed in section (5.1), has never been addressed, and security module is an essential requirement.

All of the reviewed reputation-based approaches implement a distributed architecture, and use first- and second-hand observation to evaluate the cooperation in the network. However, only Buchegger and Boudec [11] evaluate the trustworthiness of the second-hand observation. Regarding the reaction to selfish misbehavior, isolation of selfish nodes is more preferred than avoidance as it serves as a punishment for the selfish nodes. Although the approaches can improve network throughput, they face two problems, which are, they require a unique identity for each node and prone to false detection.

The reviewed game-based approaches also implement a distributed architecture. They implement either per-node or per-session monitoring. Unlike the per-node monitoring, the per-session monitoring does not require every node to have a unique identity. They, however, never address the problem of imperfect monitoring whereby the nodes may acquire the wrong information from the environment. Moreover, most of them require domain knowledge, such as the number of nodes in the network, to function properly. Furthermore, if they are using per-node monitoring, they have to maintain the knowledge on a per-node basis.

After reviewing the related work, it appears that most of the problems in the reputation-based and game-based approaches, such as the prerequisite of perfect monitoring and a unique identity linked to the behavior of each node in the network, arise from the requirement of maintaining memory of past interactions. For example, in the reputation-based system, the memory of past interactions is maintained in the form of reputation values.

This requirement exists because the existing approaches are based on the principle of reciprocity. The principle implies that where there are repeated interactions, a cooperative or selfish behavior will be repaid in the next interaction directly or indirectly. Direct reciprocity refers to a situation where an individual’s action will be repaid by the recipient of his action [23]. Indirect reciprocity, on the other hand, refers to a situation where the individual’s action to the recipient will be repaid by a third party whom observes the interaction [24]. The existing approaches utilize these kinds of reciprocity in order to enforce cooperation. However, in MANETs where the nodes join and leave the networks freely, there is a possibility that a node never meets the same nodes again or a third party has no chance to interact with a node whose interactions with other nodes have been observed by the third party. In these situations, there is no reciprocity to utilize and the existing approaches such as the reputation-based approaches may not be effective.

To address the problem, the requirement of memory of past interactions must be removed, in other words cooperation without reciprocity needs to be investigated.

6. TAG-BASED COOPERATION

Cooperation without reciprocity has been investigated by researchers and the common idea they share is the use of tag-based mechanisms to enforce cooperation. They show, using computer simulations, that high cooperation can be produced and sustained from the mechanisms [25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35]. They, however, only consider stationary environment where nodes have fixed positions such as donation scenario [32] and peer-to-peer networks (P2P) [28]. In contrast, we investigate the use of such mechanisms in mobile environment such as MANETs. Tag-based mechanisms can be used to solve the problem mentioned in Section (5.4) as they do not require keeping memory of past interactions such as observation logs and reputation records. In the following, we discuss the background and related work of tag-based cooperation.

To demonstrate the principle of a tag-based cooperation, consider a population in which each agent has a tag. Agents with identical tags are perceived as a local interaction group. Thus, the population is partitioned into groups of different tags. If all the agents in a group always choose to cooperate within the group while agents in another group always choose to defect, then the cooperative agents will gain higher average payoffs than the selfish agents. Assuming all agents always try to maximize their own payoffs, the cooperative agents will have higher reproduction than the selfish agents. Subsequently, the cooperative agents will take over the population [28].

Previous models have investigated the effects of different variables on the emergence and maintenance of tag-based cooperation in order to determine the factors or conditions that can foster high cooperation. The variables include mutation rates [28, 34], tag and strategy linkage [36], agents dispersal and cost to benefit ratio [29], incomplete social information [37] and space and population structures [25, 34, 38].

6.1 Characteristics of a Tag-based Cooperation Enforcement Model

This section lists the characteristics of tag-based cooperation enforcement model. In our view, there are three main characteristics of the model i.e., tags, interactions and agents.

6.1.1 Tags

Tags, in the context of tag-based cooperation, are observable traits or markings that are attached to individuals [39]. Examples of tags include, but not limited to, an individual's style of cloth that can be used to determine the social group of the individual [28] or the visible patterns on animals which assist the selective mating process between them [39]. In computational models, these tags can be represented by real numbers [32] or bit strings [28], and they need to evolve in order to structure interactions between the agents [39].

6.1.2 Interactions

How agents interact among them is guided by the rules of interactions defined for the system. The rules of interactions of a tag-based system include type of scenario that the agents are playing, conditions that determine whether an agent cooperates or defects, payoffs that define the costs and benefits of cooperation and defection and how tags and strategies of agents evolve in the population.

6.1.3 Agents

Each agent has a tag, strategies on how to interact with other agents and attributes such as its mobility and view range. The view range refers to whether an agent has limited or unlimited coverage of the population. An unlimited coverage gives an agent the chance to interact with any agent in the population while limited coverage limits its interaction with only agents within its view range.

6.2 Review of Existing Tag-based Cooperation Enforcement Models

The reviews focus on the tag, interaction and agent characteristics of the existing tag-based cooperation enforcement models. Here we only include a sample of representative approaches that are important to our work, although the literature on tag-based models is extensive.

6.2.1 Riolo et al.

Riolo et al. [32] proposed a tag-based cooperation approach in which an agent decides to cooperate with another agent only if their tags are sufficiently similar. They demonstrated their approach using a donation scenario. In the scenario, each agent plays as a potential donor and interacts with a set of randomly chosen neighbors in the population.

Each agent has a tag, τ and a tolerance threshold, T which are randomly assigned and uniformly sampled from [0, 1]. For instance, an agent A donates to a potential recipient B only if

$$|\tau_A - \tau_B| \leq T_A \tag{4}$$

where T_A is A's tolerance threshold. A donor pays a cost, c if it decides to donate (or cooperate) and the recipient receives a benefit, b. All agents are given the same number of pairings to donate in a generation. After all agents have played the donation session in a generation, each agent is compared with another random agent from the population. Agents with higher scores produce more offsprings than agents with lower scores. Each offspring's tag and tolerance are subject to mutation with low probability. A mutation gives a new value of tag to an offspring and adds noise to its tolerance.

The model involves stationary agents that have complete view of the population (i.e. agents can be paired with any other agents from the population).

6.2.2 Hales and Edmonds

In Hales and Edmonds' approach [28], they interpret tag as the neighbor list stored in each node, meaning that nodes which have the same neighbor list can be considered as an interaction group. Their idea is that each node plays a single round of Prisoner's Dilemma game with a randomly chosen neighbor. Then it will compare its payoff with a random node from the population. If its payoff is lower than the other node, it removes its entire neighbor, connects to the other node and its neighbors, and copies the other node's strategy. In evolutionary perspective, this process represents the reproduction of agent with better fitness. Figure 2(a) and 2(b) illustrate the scenario before and after node *A* performed the reproduction process based on node *B*, respectively. They also applied their approach in a simulation of P2P file-sharing scenario.

Similar to the model proposed by Riolo et al., Hales and Edmonds' model also involves stationary agents that have complete view of the network.

6.2.3 Griffiths and Luck

Griffiths and Luck [27] adopted the model proposed by Riolo et al. but with the addition of neighborhood context assessment and biased modification of connections to neighbors. They used a donation scenario similar to Riolo et al. in order to evaluate their approach. However, unlike the previous two models, they included the presence of agents that are unconditionally selfish (i.e. agents that accepts donation from others but never donate).

The neighborhood context assessment requires each agent to observe the behavior of its neighbors. An agent increases or decreases a neighbor's context assessment value by one if the neighbor cooperates or defects, respectively. By including the context assessment, the condition in which an agent *A* donates to agent *B* changes from eq. (4) to

$$|\tau_A - \tau_B| \le (1-\gamma).T_A + \gamma.C_A \qquad (5)$$

where C_A is the average of context assessment values of agent *A*'s neighbors and γ is the weight of the context assessment. After all agents have interacted with their pairs in a generation, each agent compares its score with another random agent from the population. If its score is lower than the other agent, it copies the other agent's tag and tolerance and modifies its neighborhood connections. The modification of neighborhood connections involves disconnecting a proportion of neighbors that have the lowest context assessment values and replacing them with better-performing neighbors from the compared agent.

Same as the previous two models, this model also involves stationary agents that have complete view of the population (i.e. an agents can compare itself with any random agent from the population).

6.3 Analysis of Tag-based Cooperation Enforcement Models

Although they have showed that their tag-based approaches can lead to the emergence of high cooperation (as high as: 79% donation rate [32]; 90% donation rate [27]; and 99% cooperation [28]) there are several issues that need to be discussed.

First, all of the reviewed models only consider stationary environment in which agents are not mobile. The agents also have complete view of the population. In MANET, the situation is different. For instance, if we consider MANET scenario in which nodes are mobile and have partial view of the network, which is limited by their transmission range (refer fig. 2(c)), the reproduction process similar to fig. 2(a) and 2(b) could happen only if node *B* and its neighbor are in node *A*'s transmission range (refer fig. 2(d)). However, in a mobile environment, there are many possibilities of nodes' positions because the topology changes frequently. For instance, if only node *B* moves into node A's transmission range while its neighbors are outside the range (refer fig. 2(e)), the same process cannot not be done. To the best of our knowledge, the effect of nodes' mobility on tag-based mechanisms has never been explored. Therefore, it is in our interest to investigate the use of such mechanisms in a mobile environment such as MANETs.

Second, in the model proposed by Riolo et al., agents with similar tags are assumed to help each other. Henrich [40] argued that this assumption creates a population of cooperators instead of mixed population of cooperators and defectors (or selfish agents). In order to remove this biased assumption, Hammond and Axelrod [29] suggested that each agent possess two traits of strategy i.e., cooperate or defect when interacting with agents that have the same tag and cooperate or defect when interacting with agents that have different tag. By having these traits, there will be agents that receive cooperation from others of the same tag but always defecting. These agents can be classified as selfish.

Third, the context assessment proposed by Griffiths and Luck can be viewed as maintaining memory of past interactions. As a consequence, it will have the same problems as existing reputation-based systems such as requiring perfect monitoring of agents and a unique identity linked to the behavior of each agent, as discussed previously in section (5.4).

All of these issues need to be considered when designing a tag-based cooperation enforcement model for MANETs.

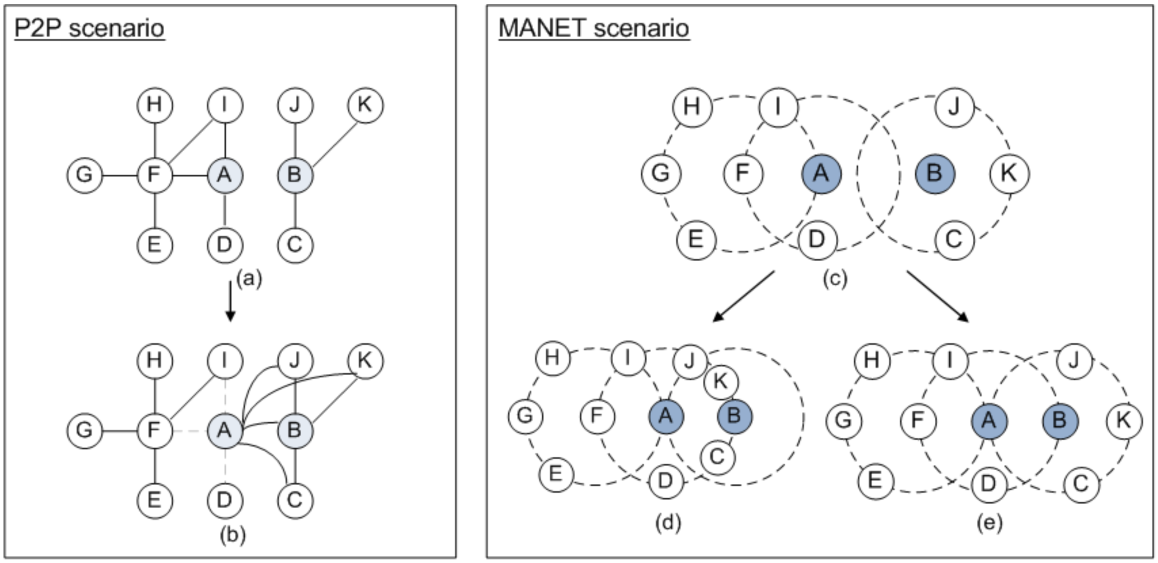

Figure 2: Comparison Between P2P And MANET Scenarios Using Hales and Edmonds' Approach

7. CONCLUSION

This paper presented a number of cooperation enforcement models targeting MANETs. The models were investigated with regards to the generic characteristics of a cooperation enforcement model and characteristics specific to their types of approach. The models were then analyzed to find their problems. We found that most of the problems of existing cooperation enforcement models for MANETs arise from the requirement of maintaining memory of past interactions. In order to address the problem, tag-based cooperation enforcement models, which does not require maintaining memory of past interactions, were introduced and discussed. A number of tag-based cooperation enforcement models were reviewed with regards to the characteristics of a tag-based cooperation enforcement model and their issues in relation to implementing them in MANETs were discussed. We are currently developing a tag-based cooperation enforcement model. Our preliminary results show that it has the capability to increase cooperation rate between mobile agents [41].

REFERENCES:

[1] Ismail, Z., Hassan, R. (2010). Performance of AODV routing protocol in mobile ad hoc network. In *Proceedings of International Symposium in Information Technology (ITSim 2010)*, (pp. 1-5). Kuala Lumpur, Malaysia.

[2] Ismail, Z., Hassan, R. (2011). A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET. In *Proceedings of 17th Asia-Pacific Conference on Communications (APCC 2011)*, (pp. 637-642). Kota Kinabalu, Malaysia.

[3] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom 2000)*, (pp. 255-265). Boston, MA, USA.

[4] Michiardi, P., & Molva, R. (2002). Simulation-based analysis of security exposures in mobile ad hoc networks. In *Proceedings of the European Wireless Conference 2002*. Florence, Italy.

[5] Buttyan, L., & Hubaux, J.-P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM/Kluwer Mobile Networks and Applications*, *8*(5), (pp. 579-592).

[6] Buttyan, L., & Hubaux, J.-P. (2001). Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks. Tech. Rep. No. DSC/2001/001, Swiss Federal Institution of Technology, Lausanne, Switzerland.

[7] Anderegg, L., & Eidenbenz, S. (2003). Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In *Proceedings of the 9th ACM Annual International Conference on Mobile Computing and Networking (MobiCom 2003)*, (pp. 245-259). New York City, NY, USA.

[8] Buttyan, L., & Hubaux, J.-P. (2000). Enforcing service availability in mobile ad-hoc WANs. In *Proceedings of The First ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2000)*, (pp. 87-96). Boston, MA, USA.

[9] Yoo, Y., Ahn, S., & Agrawal, D. P. (2005). A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks. In *Proceedings of the 2005 IEEE International Conference on Communications (ICC 2005)*, (pp. 3005-3009). Seoul, Korea.

[10] Zhong, S., Chen, J., & Yang, Y. R. (2003). Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, (pp. 1987-1997). San Francisco, CA, USA.

[11] Buchegger, S., & Le Boudec, J.-Y. (2002). Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In *Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking and Computing (MobiHoc 2002)*, (pp. 226-236). Lausanne, Switzerland.

[12] Michiardi, P., & Molva, R. (2002). CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, (pp. 107-121). Portoroz, Slovenia.

[13] Miranda, H., & Rodrigues, L. (2003). Friends and foes: preventing selfishness in open mobile ad hoc networks. In *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCS 2003)*, (pp. 440-445). Providence, RI, USA.

[14] Osborne, M. J., & Rubinstein, A. (1997). *A course in game theory*. Cambridge, MA, USA: MIT Press.

[15] Felegyhazi, M., Hubaux, J.-P., & Buttyan, L. (2006). Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, *5*(5), (pp. 463-476).

[16] Srinivasan, V., Nuggehalli, P., Chiasserini, C. F., & Rao, R. R. (2003). Cooperation in wireless ad hoc networks. In *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, (pp. 808-817). San Francisco, CA, USA.

[17] Urpi, A., Bonuccelli, M., & Giordano, S. (2003). Modelling cooperation in mobile ad hoc networks: a formal description of selfishness. In *Proceedings of the Workshop Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOPT 2003)*, (pp. 303-312). Sophia-Antipolis, France.

[18] Yu, W., & Liu, K. J. R. (2007). Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, *6*(5), (pp. 507-521).

[19] Nash, J. (1951). Non-cooperative games. *The Annals of Mathematics*, *54*(2), (pp. 286-295).

[20] Huang, E., Crowcroft, J., & Wassell, I. (2004). Rethinking incentives for mobile ad hoc networks. In *Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems (PINS '04)*, (pp. 191-196). Portland, OR, USA.

[21] Douceur, J. R. (2002). The sybil attack. In *Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002)*, (pp. 251-260). Cambridge, MA, USA.

[22] Yau, P.-W., & Mitchell, C. J. (2003). Reputation methods for routing security for mobile ad hoc networks. In *Proceedings of Joint First Workshop on Mobile Future and Symposium on Trends in Communications (SympoTIC 2003)*, (pp. 130-137). Bratislava, Slovakia.

[23] Trivers, R. L. (1971). The evolution of reciprocal altruism. *The Quarterly Review of Biology*, *46*(1), (pp. 35-57).

[24] Alexander, R. D. (1987). *The biology of moral systems*. Piscataway, NJ, USA: Aldine Transaction.

[25] Antal, T., Ohtsuki, H., Wakeley, J., Taylor, P. D., & Nowak, M. A. (2009). Evolution of cooperation by phenotypic similarity. *Proceedings of the National Academy of Sciences of the United States of America*, *106*(21), (pp. 8597-8600).

[26] Axelrod, R., Hammond, R. A., & Grafen, A. (2004). Altruism via kin-selection strategies that rely on arbitrary tags with which they coevolve. *Evolution*, *58*(8), (pp. 1833-1838).

[27] Griffiths, N., & Luck, M. (2010). Changing neighbours: improving tag-based cooperation. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, (pp. 249-256). Toronto, Canada.

[28] Hales, D., & Edmonds, B. (2005). Applying a socially inspired technique (tags) to improve cooperation in P2P networks. *IEEE Transactions on Systems, Man, and Cybernetics*, *35*(3), (pp. 385-395).

[29] Hammond, R. A., & Axelrod, R. (2006). Evolution of contingent altruism when cooperation is expensive. *Theoretical Population Biology*, *69*(3), (pp. 333-338).

[30] Hammond, R. A., & Axelrod, R. (2006). The evolution of ethnocentrism. *Journal of Conflict Resolution*, *50*(6), (pp. 926-936).

[31] Ihara, Y. (2011). Evolution of culture-dependent discriminate sociality: a gene-culture coevolutionary model. *Philosophical Transactions of the Royal Society B*, *366*(1566), (pp. 889-900).

[32] Riolo, R. L., Cohen, M. D., & Axelrod, R. (2001). Evolution of cooperation without reciprocity. *Nature*, *414*(6862), (pp. 441-443).

[33] Shultz, T. R., Hartshorn, M., & Hammond, R. A. (2008). Stages in the evolution of ethnocentrism. In *Proceedings of the 30th Annual Conference of the Cognitive Science Society*, (pp. 1244-1249). Austin, TX, USA.

[34] Spector, L., & Klein, J. (2006). Genetic stability and territorial structure facilitate the evolution of tag-mediated altruism. *Artificial Life*, *12*(4), (pp. 553-560).

[35] Traulsen, A., & Schuster, H. G. (2003). Minimal model for tag-based cooperation. *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, *68*(4), 046129.

[36] Jansen, V. A. A., & Baalen, M. V. (2006). Altruism through beard chromodynamics. *Nature*, *440*, (pp. 663-666).

[37] Masuda, N., & Ohtsuki, H. (2007). Tag-based indirect reciprocity by incomplete social information. *Proceedings of the Royal Society B: Biological Sciences*, *274*, (pp. 689-695).

[38] Lehmann, L., & Perrin, N. (2002). Altruism, dispersal, and phenotype-matching kin recognition. *American Naturalist*, *159*(5), (pp. 451-468).

[39] Holland, J. H. (1995). *Hidden order: how adaptation builds complexity*. New York, NY, USA: Addison-Wesley.

[40] Henrich, J. (2004). Cultural group selection, coevolutionary processes and large-scale cooperation. *Journal of Economic Behavior and Organization*, *53*(1), (pp. 3-35).

[41] Othman, N.E., & Weber, S. (2011). Towards Tag-based cooperation for mobile ad hoc networks. In *Proceedings of the 30th IEEE Symposium on Reliable Distributed Systems Workshops (SRDSW 2011)*, (pp. 20-25). Madrid, Spain.

APPENDIX:

Table 1: Comparison Between Existing Cooperation Enforcement Approaches

Types	Approach	Management		Features				Issues		
Credit-based		Centralized	Distributed	Payment model		Payment security		Scalability	Excessive credits	Security module
				Source -based	Destination -based	Local hardware	Credit server			
	Anderegg and Eidenbenz	Yes	No	Yes	No	No	Yes	Low	Yes	Yes
	Buttyan and Hubaux	No	Yes	Yes	No	Yes	No	High	Yes	Yes
	Yoo et al.	Yes	No	Yes	Yes	No	Yes	Low	Yes	Yes
Reputation-based	Zhong et al.	Yes	No	Yes	No	No	Yes	Low	Yes	Yes
		Centralized	Distributed	Observation		Reaction		Unique identity	Prone to false detection	Punish selfish nodes
				First-hand	Second-hand	Avoidance only	Isolation			
	Buchegger and Boudec	No	Yes	Yes	Yes, trusted	No	Yes	Yes	Yes	Yes
	Marti et al.	No	Yes	Yes	Yes, non-trusted	Yes	No	Yes	Yes	No
	Michiardi and Molva	No	Yes	Yes	Yes, non-trusted	No	Yes	Yes	Yes	Yes
Game-based		Centralized	Distributed	Monitoring		Network scenario		Unique identity	Perfect monitoring	Domain knowledge
				Per-node	Per-session	Static ad-hoc network	MANET			
	Felegyhazi et al.	No	Yes	No	Yes	Yes, with topology	No	No	Yes	No
	Srinivasan et al.	No	Yes	No	Yes	Yes, without topology	No	No	Yes	Yes, total number of nodes
	Yu and Liu	No	Yes	Yes	No	No	Yes, noisy and hostile	Yes	Yes	Yes, knowledge per node