Enforcing Cooperation between Nodes in Mobile Ad hoc Networks

Nor Effendy Othman

A thesis submitted to the University of Dublin, Trinity College

in fulfillment of the requirements for the degree of

Doctor of Philosophy (Computer Science)

2013

Declaration

I, the undersigned, declare that this thesis has not been submitted as an exercise for a degree at this or any other university, and that unless otherwise stated, it is entirely my own work.

I agree to deposit this thesis in the University's open access institutional repository or allow the library to do so on my behalf, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement.

Nor Effendy Othman

Dated: October 1, 2013

Summary

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.

A mobile ad hoc network 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 mobile ad hoc network rely on multi-hop communication to communicate with nodes outside their transmission ranges. For example, if a destination node is out of a source node's direct transmission range, nodes between them need to act as routers, forwarding packets from the source to the destination. 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.

Nodes in mobile ad hoc networks for military or emergency operations belong to the same authority and have the same goals; thus they are self-motivated to cooperate with each other to ensure the success of their operations. In self-organized mobile ad hoc networks such as civilian mobile ad hoc networks, however, 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 mobile ad hoc networks; however, most of them require each node to maintain memory of past interactions. This requirement can be a significant problem in open and large mobile ad hoc networks. To address this problem, the requirement of memory of past interactions must be removed; in other words cooperation without reciprocity needs to be achieved. Cooperation without reciprocity has been investigated by researchers from a number of fields and the common idea they share is the use of tag-based mechanisms to enforce cooperation.

This thesis introduces MaTaCo, a mobility-aware tag-based cooperation enforcement system, which enables cooperation enforcement without requiring each node to maintain memory of past interactions, for mobile environments and MANETs. The principal contribution is two-fold. First, compared to existing cooperation enforcement approaches for MANETs, our approach does not require keeping memory of past interactions such as observation logs and reputation records. Hence, there is no need for each node to have a monitoring mechanism and a unique identity linked to the behavior of each observed node. Second, compared to existing tag-based models, our models take into account the mobility of nodes and their limited transmission range. Therefore, our models are suitable for applications whereby the agents in the environment are moving and have incomplete information about the environment.

MaTaCo is implemented in an agent-based simulator and a network simulator. It is compared to existing tag-based approaches. The evaluations show that our approach promotes higher cooperation between mobile agents or nodes than existing tag-based system and has the capability to respond and adapt to changing mobile environment.

Acknowledgements

First and foremost, I would like to express my gratitude to my supervisor, Prof. Dr. Stefan Weber, for his support and guidance over the years. His enthusiasm and kindness have inspired me the whole time and never wasted.

I gratefully acknowledge the financial support from the Ministry of Higher Education Malaysia and Universiti Kebangsaan Malaysia.

I thank all members of Distributed Systems Group for the great and enjoyable working environment, and the fruitful discussions, which helped to guide my work.

Last but not least, a special appreciation to my family. Their never ending support has made my Ph.D. journey more meaningful.

Nor Effendy Othman
University of Dublin, Trinity College
October 2013

Publications Related to this Ph.D.

- 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, October 2011.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This thesis presents a new approach to cooperation enforcement in mobile ad hoc networks (MANETs) using tag-based cooperation. We specifically focus on the problem of cooperation in packet forwarding in MANETs. In our approach, the mobility of a node is incorporated in its tag. Each node selects its forwarding strategy based on its tag similarity with its neighbors. Nodes respond and adapt to changing mobile environment by evaluating whether their neighbors have similar tags and selecting their forwarding strategy, respectively, based on the relative mobility between them and their neighbors. The novelty of our approach stems from its decentralized tag-based cooperation enforcement scheme that is mobility-aware and does not rely on memory of past interactions. By providing such a scheme that is responsive and adaptive to changing mobile environment, we aim to reduce the advantage of selfish nodes and thus increase cooperation between nodes in MANETs.

This chapter introduces MANET including its historical background, applications, characteristics and challenges. The term cooperation is defined and cooperation domains in ad hoc networks are introduced. Furthermore, we present the motivation for this work. We also present the contributions of this thesis and outline the rest of this thesis.

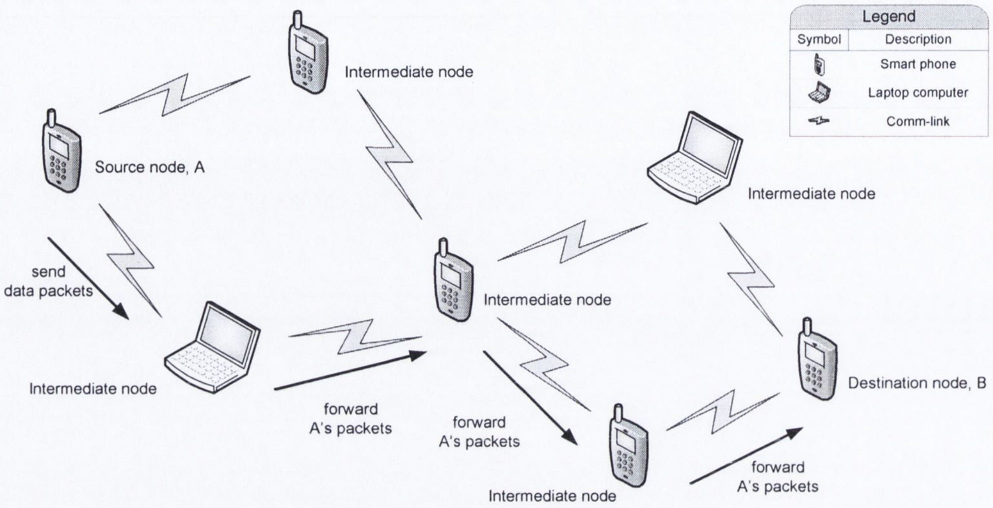

Figure 1.1: An example of a mobile ad hoc network

1.1 Background

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. Thus, cooperation between nodes is necessary to establish an operational network. Figure 1.1 illustrates an example of a mobile ad hoc network.

The basic idea of mobile ad hoc networks emerged as early as 1973 when Defense Advanced Research Projects Agency (DARPA) initiated research that was motivated by the need to provide computer communications in a mobile environment [Jubin & Tornow (1987)]. At the time, they were known as Packet Radio Networks (PRNET). PRNET were primarily intended for military applications e.g. to support distributed, survivable command, control, and communications in battlefield [Frankel (1982)]. As the technology progressed, the applications of mobile ad hoc network have been extended to include disaster relief and emergency operations. Moreover, commercial and civilian applications of mobile ad hoc networks have been envisioned as well [Blazevic et al. (2001)]. Examples of commercial and civilian applications include the provision of wireless connectivity in remote areas, vehicular ad hoc networks and wireless sensor networks.

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. Mobile ad hoc networks 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 which nodes freely join and leave the network frequently, results in frequently changing topology. Hereby decreasing the stability of the links and routes. 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 [Buttyan & Hubaux (2003)].

1.1.1 Cooperation in Mobile Ad hoc Networks

In mobile ad hoc networks, nodes rely on multi-hop forwarding to communicate with each other out of their transmission ranges. Cooperation between nodes, i.e. forwarding packets for each other, is necessary to achieve multi-hop communication. This section first describes the concept of cooperation particularly in the case of ad hoc networks and then discusses the problem of selfish misbehavior. Figure 1.2 presents the overview of this section.

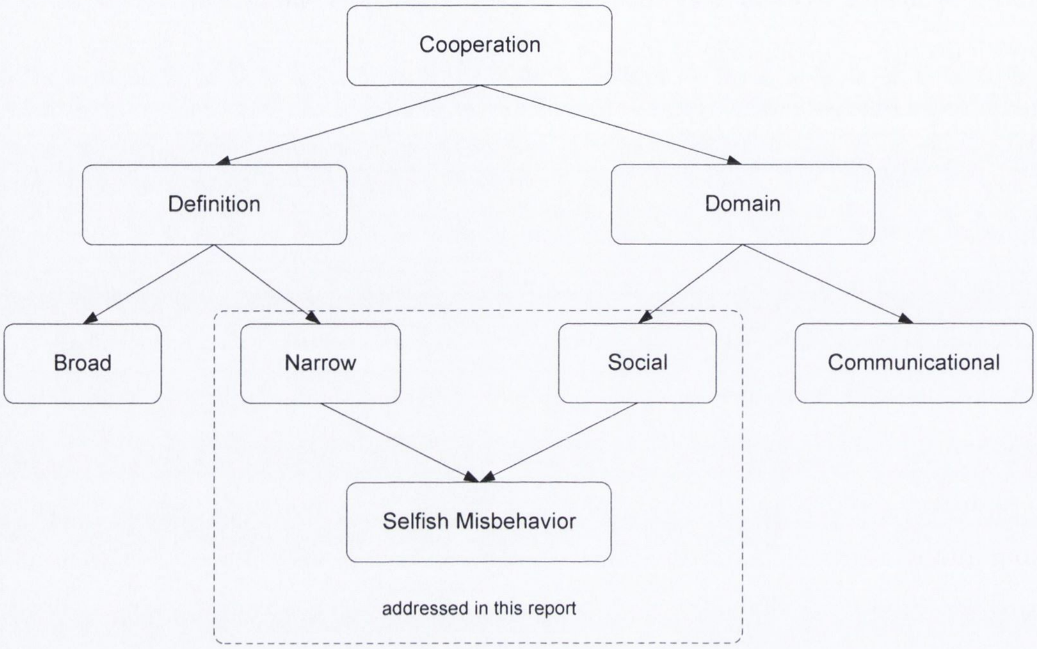

Figure 1.2: Overview of cooperation in mobile ad hoc networks

1.1.1.1 Defining Cooperation

The term cooperation implies the idea of working together. Richerson et al. [Richerson et al. (2003)] define cooperation in two ways:

> "Cooperation has a broad and a narrow definition. The broad definition includes all forms of joint action by two or more individuals. The narrow definition is restricted to situations in which joint action poses a dilemma for at least one individual such that, at least in the short run, that individual would be better off not cooperating."

The narrow definition is closer to our interest than the broad definition. In the case of packets forwarding in mobile ad hoc networks, each node is tempted to drop packets it should forward, as this would save some of its resources e.g. battery power and bandwidth. If all nodes reason in the same way, however, no packets will reach their destinations. On the other hand, nodes could do better by mutually relaying each other's packets, but they may lose some resource.

Hence, they face a *forwarder's dilemma* [MacKenzie & DaSilva (2006)]. The forwarder's dilemma exists in one of the cooperation domains in ad hoc networks, i.e. social cooperation domain. In the following, we distinguish between the cooperation domains.

1.1.1.2 Cooperation Domains in Ad hoc Networks

Two distinct domains of cooperation exist in ad hoc networks, namely communicational cooperation and social cooperation [Mähönen et al. (2006)].

Communicational Cooperation Communicational cooperation deals with the provision of cooperative communication protocols and transmission methods to enhance network performance and improve the utilization of resources. Techniques such as network coding, cooperative coding, cooperative diversity and cooperative antennas are extensively studied to address the problems of communicational cooperation.

Social Cooperation Social cooperation refers to nodes participation in packet forwarding. Each node ultimately decides whether to cooperate or not. In closed ad hoc network applications e.g. military or disaster relief networks, social cooperation can be guaranteed as nodes in the network share the same goals. They are self-motivated to cooperate with each other to ensure successful mission accomplishment. In civilian applications of ad hoc network, however, it is not obvious for nodes to cooperate with each other as they belong to different authorities and have different goals. Researchers are actively investigating on how to establish and maintain a network of cooperative nodes e.g. wireless communication devices, as well as how to encourage intermediate nodes to cooperate on forwarding packets from source to destination in a civilian context [Chen et al. (2011); Janzadeh et al. (2009); Jaramillo & Srikant (2007); Kusyk et al. (2011); Li et al. (2010); Liu et al. (2011); Lu et al. (2008); Mahmoud & Shen (2011, 2012, 2013); Wang et al. (2010); Wei & Liu (2008); Yu & Liu (2007); Zhang et al. (2007)]. The work described in this thesis falls in the social cooperation domain. Next, we discuss the motivation for this work and selfish misbehavior which is a serious threat to social cooperation.

1.2 Motivation

Selfish misbehavior refers to an act of reluctance 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 [Marti et al. (2000)].

Michiardi and Molva [Michiardi & Molva (2002b)] 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 [Buttyan & Hubaux (2003)] 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 [Buttyan & Hubaux (2001); Marti et al. (2000); Michiardi & Molva (2002b)]. It can cause problems such as throughput degradation, increasing latency and network partition. For example, Marti et al. [Marti et al. (2000)] 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 [Buttyan & Hubaux (2001)] show that the misbehavior will cause a higher throughput degradation rate in larger networks.

In self-organized MANETs such as civilian MANETs, nodes cannot be authenticated to each other as there are neither common authentication services nor a globally acceptable public key infrastructure (PKI). Applying a PKI in self-organized MANETs is not always feasible as it requires maintaining a certificate authority (CA), a central trusted third party. This contradicts with the nature of MANETs which lack of any established infrastructure. Moreover, the transmission and storage overheads of public key certificates (PKCs) in a PKI are heavy for mobile nodes with limited computing and communicational capacity [Zhao et al. (2012)]. Due to PKI's disadvantages, identity-based cryptography (IBC) has been considered as the main candidate for providing security in MANETs as it does not require a CA and its storage and communication overheads are much lower than a PKI [Zhang et al. (2006)]. However, recent work indicates that IBC is only suitable for closed MANETs such as military and public safety MANETs because it requires an administrator to distribute system parameters to all nodes before the network starts up [Zhao et al. (2013)]. As there is no global authority to enforce policies in self-organized MANETs, a mechanism is needed to defend against selfish misbehavior in the networks. This mechanism is referred as cooperation enforcement system. The main idea of the existing approaches is to provide incentives for nodes to forward packets not of direct interest to themselves. Different cooperation enforcement systems have been proposed to provide incentive for selfish nodes to cooperate. In the existing approaches, three types of incentive are used i.e. reward, punishment and necessity. Credit- and reputation-based approaches utilize reward and punishment as incentives, respectively, while game- and anonymity-based approaches use necessity as incentive.

In credit-based systems [Anderegg & Eidenbenz (2003); Buttyan & Hubaux (2000, 2003); Yoo et al. (2005); Zhong et al. (2003)], 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. However, the existing credit-based schemes 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.

In reputation-based schemes [Buchegger & Le Boudec (2002); Marti et al. (2000); Michiardi & Molva (2002a); Miranda & Rodrigues (2003)], 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. However, the major drawback of reputation-based schemes lies in the reputation records. Each reputation record stored in a node is linked to a unique identity. Thus, reputation-based schemes 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 the Sybil attack [Douceur (2002)].

Game theory has also 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 [Felegyhazi et al. (2006); Srinivasan et al. (2003); Urpi et al. (2003); Yu & Liu (2007)]. Game theory is a collection of models which can be used to study the interaction between decision-makers [Osborne & Rubinstein (1997)]. 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. However, some of existing approaches assume perfect monitoring of nodes in the networks. As perfect monitoring is not always available [Yu & Liu (2007)], recent work has considered scenarios of noisy and imperfect monitoring that are caused by transmission errors or false-positive observation in which a node is observed to forward a packet but actually has dropped it [Ji et al. (2010); Wei & Liu (2008)].

In anonymity-based schemes [Song & Zhang (2009); Sundaramurthy & Belding-Royer (2003)] the true destination of packets is hidden from intermediate nodes and destination node. Therefore, it is necessary for them to be cooperative, i.e. forwarding packets that they receive, because there is a possibility that the packets are destined for them. If they choose to be selfish, i.e. dropping packets that they receive, then they risk losing packets that are destined for them. This type of schemes use encryption techniques to conceal the true destination of packets and they depend on the existence of PKI system in order to successfully encrypt the packets.

1.3 Thesis Aims and Objectives

The limitations of existing cooperation enforcement approaches motivate the research question addressed by this thesis, which is: what techniques and properties are necessary from a cooperation enforcement model, targeting MANETs, to increase cooperative nodes and reduce selfish nodes. In particular, this thesis addresses the challenge of enforcing cooperation in packet forwarding in the presence of mobile nodes.

To address this question, this thesis proposes MaTaCo, a mobility-aware tag-based cooperation enforcement model for MANETs. MaTaCo incorporates a mobility metric in its mechanism which allows each node to measure its tag similarity to its neighbor's based on their relative mobility. This gives nodes the ability to respond and adapt to changing mobile environment in MANETs. MaTaCo aims to achieve an objective of increasing cooperation between nodes in MANETs by increasing nodes cooperation rate and the number of cooperative nodes in a MANET, which in turn increase the packet delivery ratio of the network.

1.4 Contributions

The cooperation enforcement approach described in this thesis contributes to the state of the art in the area of cooperation enforcement approaches for MANETs in the following points:

- The proposed approach adds a new class of cooperation enforcement approaches for MANETs. Existing models for MANETs can be classified as credit-, reputation-, game- and anonymity-based approaches, while the approach proposed in this thesis can be classified as a tag-based model; which is novel for this type of networks.

- Compared to existing cooperation enforcement approaches for MANETs, the proposed approach does not require keeping memory of past interactions such as observation logs and reputation records. Hence, there is no need for each node to have a monitoring mechanism and a unique identity linked to the behavior of each node.

- Compared to existing tag-based models for wired networks, the proposed approach takes into account the mobility of nodes and their limited transmission range. Therefore, the approach is suitable for applications whereby the agents in the environment are moving and have incomplete information about the environment.
- The proposed approach incorporates a mobility metric into its mechanism which makes nodes in MANETs responsive and adaptive to the non-stationary nature of MANETs.

A tag-based cooperation enforcement system that is mobility-aware named MaTaCo has been implemented. The evaluation of MaTaCo validates the advantages of a mobility-aware tag-based cooperation enforcement model over existing tag-based cooperation enforcement models, with regards to increasing cooperation rate, the number of cooperative nodes and packet delivery ratio in MANETs.

1.5 Scope

This thesis focuses on the problem of selfish nodes, not malicious nodes. Selfish nodes are passive nodes that refuse to spend their resources e.g. energy to forward others' packets. Malicious nodes, on the other hand, are active nodes that aim to disrupt network operations. It is assumed that location and velocity information is not available at each node. It should also be noted that this work assumes that in a packet forwarding session, each intermediate node selects its forwarding strategy based on the tag of preceding node, not the tag of source node.

1.6 Thesis Outline

The remainder of this thesis is organised as follows. Chapter 2 presents the state of the art in cooperation enforcement approaches for mobile ad hoc networks, with a particular emphasis on existing cooperation enforcement systems and their characteristics. Chapter 3 presents the concept of tag-based cooperation and the design of proposed approach. Chapter 4 presents the implementation of proposed approach in agent-based model and network model. Chapter 5 experimentally evaluates and validates the properties of the cooperation enforcement model presented in Chapter 3. Chapter 6 summarises and discusses future work.

1.7 Summary

This chapter outlined the goals and scope of work described in this thesis, specifically the definition of a new cooperation enforcement model that can be classified as a tag-based approach. Background information relating to mobile ad hoc networks and cooperation enforcement that is relevant for this thesis were presented and the challenges of cooperation enforcement in mobile ad hoc networks were discussed. The problem was defined in more detail by examining the limitations of existing cooperation enforcement approaches. In addition, this chapter outlined the contributions and scope of this thesis.

Chapter 2

Cooperation Enforcement in Mobile Ad hoc Networks

This thesis merges between the domains of cooperation enforcement in MANETs and tag-based approach. Therefore in this chapter, we introduce the background necessary for understanding our approach as well as related work to position our contribution and distinguish our approach from existing approaches. 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 to provide justification for applying tag-based cooperation in our approach. Then we introduce the concepts found in tag-based cooperation and review existing tag-based approaches.

2.1 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, packet 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 1.2).

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 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. The existing approaches can be classified according to the type of incentive that they utilize, i.e. reward, punishment and necessity.

2.2 General Analysis of Cooperation Enforcement Models for Mobile Ad hoc Networks

This section provides a general analysis of cooperation enforcement models targeting MANETs. Since there is no global authority to enforce policies, cooperation can only be enforced if it is in the self-interest of each participating node, i.e. through the introduction of some form of incentive. Therefore we divide existing approaches based on the three main classes of incentives i.e. reward, punishment and necessity. Figure 2.1 illustrates an overview of the general analysis of cooperation enforcement approaches. This section breaks down the general analysis of the cooperation enforcement problem based on the figure.

2.2.1 Reward

In the context of MANETs, reward serves as a recognition of cooperative behavior, i.e. forwarding packets for other nodes. The expectation of reward could motivate self-interested nodes to be cooperative in the network. The absence of reward, on the other hand, could lead them to become selfish as they would have to bear their own cost of forwarding packets for other nodes. A class of existing cooperation enforcement models targeting MANETs that utilizes reward as an incentive is credit-based model.

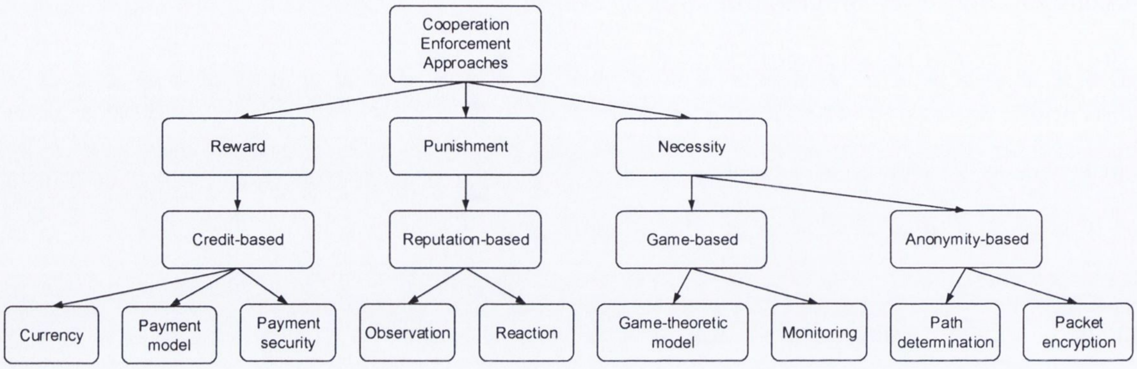

Figure 2.1: General analysis of cooperation enforcement approaches

2.2.1.1 Credit-based Model Characteristics

In credit-based models [Anderegg & Eidenbenz (2003); Buttyan & Hubaux (2000, 2003); Yoo et al. (2005); Zhong et al. (2003)], nodes receive rewards in terms of 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 currency types and payment models that regulate the dealing between nodes for packet forwarding. They also require protection modules to prevent payment fraud.

Currency Existing credit-based models can be differentiate between models that use virtual currency [Anderegg & Eidenbenz (2003); Buttyan & Hubaux (2001)] and actual currency [Yoo et al. (2005); Zhong et al. (2003)] as credit. Virtual currency is circulated within a network by including it in data packets. Thus it is managed by nodes in the network themselves. Nodes earn the virtual currency by forwarding the packets and spend it in order to send packets. On the other hand, actual currency is managed outside a network, by a third party service that manages accounts of all nodes in the network. Nodes in the network keep receipts as proofs of providing packets forwarding service. When they have fast connection to the third party service, they send the receipts to it in order to claim for payments. When it receives the receipts, it transfers payments from accounts of nodes that use the forwarding service to accounts of nodes that provide the service, accordingly.

Payment Model Most payment models proposed in the literature are based on payment per packet. Buttyan and Hubaux [Buttyan & Hubaux (2000)] 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.

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. As virtual currency is managed by nodes in a network, a security module has to be implemented at each node. On the other hand, in the case of actual currency, a third-party service can provide payment security by validating the receipts that nodes send when claiming for payment. Virtual currency counter [Buttyan & Hubaux (2003)] and centralized third-party service [Zhong et al. (2003); Yoo et al. (2005)] have been proposed to prevent payment fraud for virtual currency and actual currency, respectively.

2.2.2 Punishment

Punishment serves as a deterrent to non-cooperative behavior in MANETs, i.e. not forwarding packets for other nodes. It can be given in the form of response directed solely at non-cooperative or selfish nodes, i.e. not providing the service of forwarding packets for them. Similar to the expectation of reward, the fear of punishment could encourage self-interested nodes to participate in forwarding packets for other nodes as non-cooperative behavior would prevent them from using the network for their own benefits. Existing reputation-based models utilize punishment as an incentive to enforce cooperation between nodes in MANETs.

2.2.2.1 Reputation-based Model Characteristics

In reputation-based models [Buchegger & Le Boudec (2002); Marti et al. (2000); Michiardi & Molva (2002a); Miranda & Rodrigues (2003)], 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. Thus, punishment served as an incentive for a node to cooperate. Existing reputation-based models typically consist of two main stages i.e. observation and reaction to selfish behavior.

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 [Buchegger & Le Boudec (2002); Marti et al. (2000); Miranda & Rodrigues (2003)]. 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.

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 [Marti et al. (2000)] and isolation [Buchegger & Le Boudec (2002); Michiardi & Molva (2002a)]. With avoidance strategies, selfish nodes are avoided during packet forwarding but they are not blocked from sending their own packets, while with isolation strategies, selfish nodes are avoided and blocked from sending their own packets.

2.2.3 Necessity

Necessity is a form of incentive that enforce cooperation by taking advantage of the rationality of self-interested nodes in which they always want to maximize their own payoffs; cooperation becomes a necessity or requirement for self-interested nodes in order for them to maximize their own payoffs. Non-cooperative behavior would only minimize their payoffs. Therefore, this could motivate them to forward packets for other nodes. There are two classes of existing approaches that utilize necessity as an incentive, i.e. game-based model and anonymity-based model.

2.2.3.1 Game-based Model Characteristics

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 [Osborne & Rubinstein (1997)]. 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 [Felegyhazi et al. (2006); Srinivasan et al. (2003); Urpi et al. (2003); Yu & Liu (2007)]. They considered different network scenarios in defining the models and analyzed the models to find an equilibrium point of cooperation strategies.

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 [Nash (1951)]. 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 [Srinivasan et al. (2003)] and a self-organized mobile ad hoc network [Yu & Liu (2007)], as well as to identify the conditions that allow cooperation to exist in a static ad hoc network [Felegyhazi et al. (2006)].

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 [Felegyhazi et al. (2006); Srinivasan et al. (2003); Urpi et al. (2003)] and per-node monitoring [Yu & Liu (2007)].

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 [Felegyhazi et al. (2006); Srinivasan et al. (2003); Urpi et al. (2003)] 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.

2.2.3.2 Anonymity-based Model Characteristics

In anonymity-based models [Song & Zhang (2009); Sundaramurthy & Belding-Royer (2003)], the ultimate destination of packets is hidden from intermediate nodes that are involved in forwarding the packets. There is a possibility that a packet that a node receives for forwarding is destined for itself. If it choose to be selfish, then it risks losing the packet. Therefore each intermediate node has no choice but to forward packets that they receive. Two important characteristics of an anonymity-based model that realize cooperation enforcement are path determination and packet encryption.

Path Determination Existing anonymity-based models determines a path for a packet to traverse from its source to its final destination based on a rule, i.e. the path must include the final destination node as one of forwarders or intermediate nodes. Due to both the rule and hidden final destination of the packet, each intermediate node has the same probability of being the final destination of the packet. This forces itself to cooperate whenever it receives a packet.

Path determination also depends on the method used to transmit packets. If unicast transmission is used, then a path is chosen such that it includes at least two nodes that are capable of decrypting packets traversing the path. On the other hand, if broadcast transmission is used, all nodes on the path must be able to decrypt the packets.

Packet Encryption The purpose of packet encryption is to conceal the true destination of a packet. In existing models, before a source node sends a packet, it first encrypts the packet with the public key of destination node, followed by the public keys of some or all of

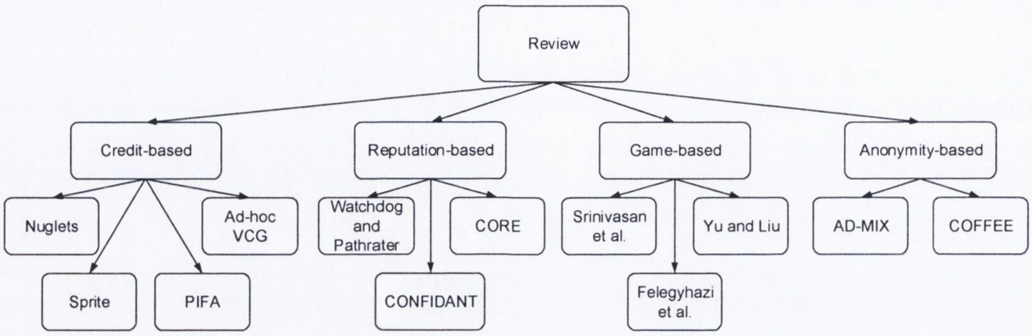

Figure 2.2: Review of existing cooperation enforcement models

the intermediate nodes on the path in a reversed order. Due to this, any source node has to know the public keys of all nodes that it plans to send its packets through. Thus, an anonymity-based model requires a PKI for key distribution.

2.3 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. For alternative approaches that have similar characteristics, we would like to point the reader to the following references: credit-based approaches [Crowcroft et al. (2004); Janzadeh et al. (2009); Lu et al. (2008); Mahmoud & Shen (2011, 2012, 2013); Zhang et al. (2007)], reputation-based approaches [Chen et al. (2011); He et al. (2004); Hu & Burmester (2006); Jaramillo & Srikant (2007); Liu et al. (2007, 2011); Refaei et al. (2005)] and game-based approaches [Altman et al. (2005); Kusyk et al. (2011); Li et al. (2010); Urpi et al. (2003); Wang et al. (2010); Wei & Liu (2008)]. Figure 2.2 shows the representative approaches that are reviewed in this section.

2.3.1 Credit-based Models

A general overview of credit-based cooperation enforcement models was provided in section 2.2.1.1. This section discusses existing credit-based models with respect to the characteristics described in section 2.2.1.1.

2.3.1.1 Nuglets

Buttyan and Hubaux proposed a virtual currency called nuglets [Buttyan & Hubaux (2001)] in their approach using decentralized management and proactive execution. Their approach operates using either PPM or PTM payment model discussed in section 2.2.1.1. 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 [Buttyan & Hubaux (2003)]. The nuglets counter, however, needs to be implemented in tamper-resistant hardware module in order to provide security and avoid modification of the counter.

2.3.1.2 Sprite

Zhong et al. proposed a model named Sprite [Zhong et al. (2003)] which operates based on centralized management and proactive execution. Sprite uses actual currency and 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 has connection to CCS. After receiving all the receipts, CCS rewards the intermediate nodes involved in the packets forwarding and charges the source node accordingly.

2.3.1.3 PIFA

Protocol Independent Fairness Algorithm (PIFA) [Yoo et al. (2005)] has centralized management and proactive execution. Its payment model is similar to Sprite where it also uses actual currency, and centralized server to manage the credits of nodes in the network and prevent

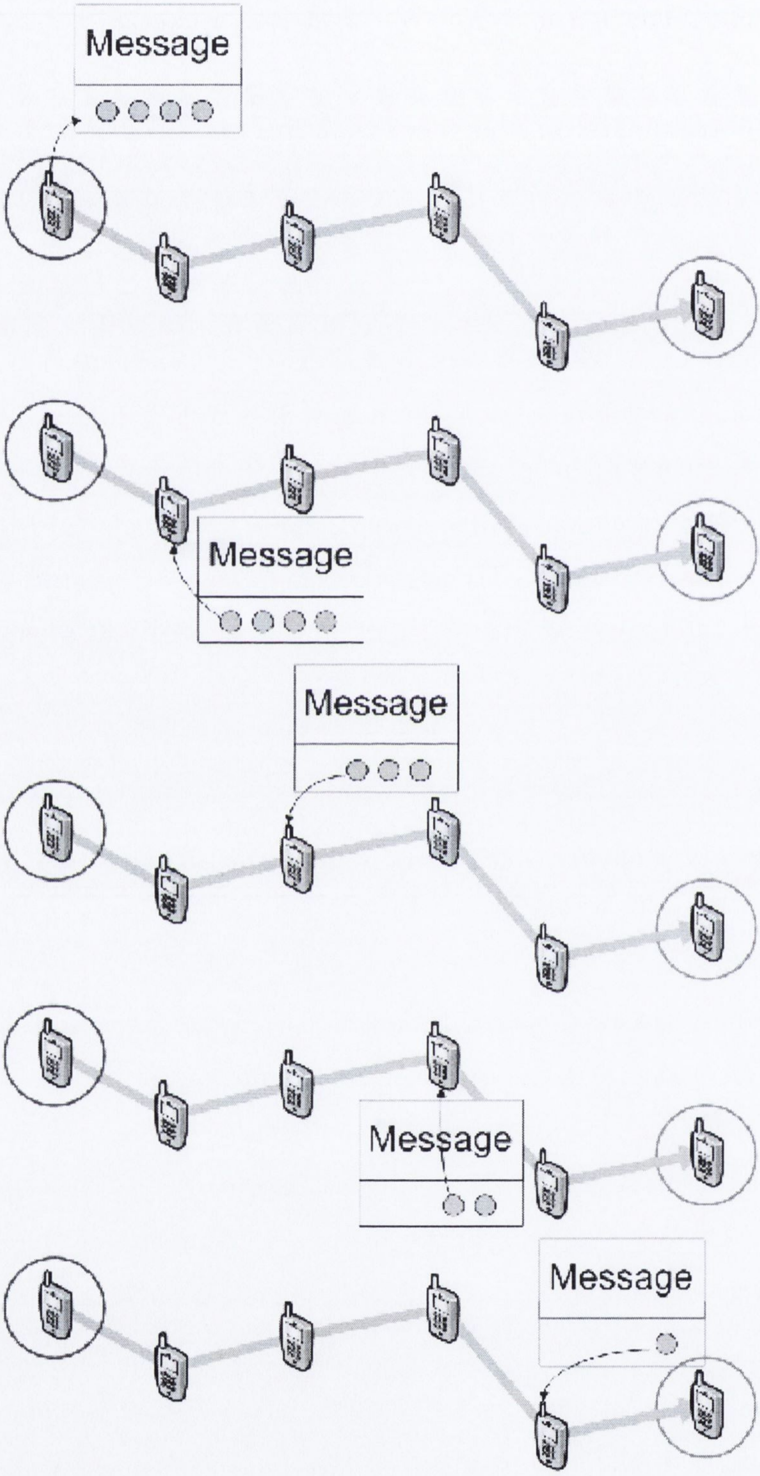

Figure 2.3: Nuglets approach: each intermediate nodes take a nuglet before forwarding to the next hop

payment fraud. The server is known as credit manager. However, PIFA is different from 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.

2.3.1.4 Ad hoc-VCG

Similar to Nuglets, Ad hoc-VCG [Anderegg & Eidenbenz (2003)] has decentralized management and proactive execution. It also uses virtual currency and 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.

2.3.2 Reputation-based Models

A general overview of reputation-based cooperation enforcement models was provided in section 2.2.2.1. This section discusses existing reputation-based models with respect to the characteristics described in section 2.2.2.1.

2.3.2.1 Watchdog and Pathrater

The watchdog and pathrater approach [Marti et al. (2000)] 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.

Watchdog and pathrater is one of the approaches that accept second-hand observation without any evaluation of trustworthiness. In this approach, second-hand observations are 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.

2.3.2.2 CONFIDANT

CONFIDANT [Buchegger & Le Boudec (2002)] 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 receive 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.

2.3.2.3 CORE

CORE [Michiardi & Molva (2002a)] 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 2.3.2.1. In CORE approach, each node classifies its observation of a node into three types of reputation:

1. Subjective reputation, that is locally calculated based on first-hand observation.

2. Functional reputation, that 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.

3. Indirect reputation, that 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.

2.3.3 Game-based Models

A general overview of game-based cooperation enforcement models was provided in section 2.2.3.1. This section discusses existing game-based models with respect to the characteristics described in section 2.2.3.1.

2.3.3.1 Srinivasan et al.

Srinivasan et al. analyzed an ad-hoc network in which the source and relay nodes are chosen randomly [Srinivasan et al. (2003)]. 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:

1. The total of its own requests relayed by others, TRR_{own}.

2. The total requests generated by itself, TRG_{own}.

3. The total of others' requests relayed by itself, TRR_{others}.

4. 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:

1. $Ratio_1 = \frac{TRR_{\text{own}}}{TRG_{\text{own}}}$

2. $Ratio_2 = \frac{TRR_{\text{others}}}{TRG_{\text{others}}}$

A node decides to relay or forward a request if:

1. $Ratio_2 < Ratio_1 + \varepsilon$, where ε is a positive real number, and

2. $Ratio_2$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. Recall from section 2.2.3.1 that 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, the existence of a Nash equilibrium motivates nodes to play the m-GTFT relay acceptance strategy as it can maximize their payoffs and consequently enforces cooperation between nodes. 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 2.2.3.1, 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.

2.3.3.2 Felegyhazi et al.

In relation to Srinivasan et al. work [Srinivasan et al. (2003)], Felegyhazi et al. argued that the random participation of source and relay nodes creates a balanced interaction pattern which is the reason unforced cooperation can emerge [Felegyhazi et al. (2006)]. 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.

2.3.3.3 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) [Yu & Liu (2007)]. 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:

1. Route participation, that is where it decide to accept or refuse route requests from other nodes.

2. Route selection, that is where it choose one of discovered routes.

3. 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:

1. 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.

2. 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.

3. 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. As discussed in section 2.3.3.1, the existence of a Nash equilibrium can guarantee nodes to follow the proposed cooperation strategy and consequently prevent them from being selfish. The reason is that nodes can maximize their payoffs when they are in a state of Nash equilibrium.

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.

2.3.4 Anonymity-based Models

A general overview of anonymity-based cooperation enforcement models was provided in section 2.2.3.2. This section discusses existing credit-based models with respect to the characteristics described in section 2.2.3.2.

2.3.4.1 AD-MIX

The AD-MIX protocol [Sundaramurthy & Belding-Royer (2003)] enforce cooperation between nodes in forwarding packets by hiding the ultimate destination of packets. It utilizes unicast transmission to transmit packets between nodes. Therefore, when a source node, S wants to send a packet to a destination node, D, S chooses two nodes, $P_1$and P_2, along a known path to D, to be polar nodes. The function of polar nodes is to decrypt the packet that is to be transmitted by S. The path from S to D also contains non-polar nodes that function as forwarders between S and P_1, P_1 and P_2, or P_2 and D. A non-polar node, can decrypt the packet only if the packet has been forwarded through $P_1$and P_2 and it is the ultimate destination of the packet. The protocol ensures that D is involved in forwarding the packet by selecting P_2beyond D. D can also be selected as P_1.

AD-MIX uses asymmetric key to encrypt and decrypt the packet. Before sending the packet, S encrypts it with the public key of D, followed by the public key of P_2 and then the public key of P_1. The transmission of the packet involves three phases, i.e.S to P_1, P_1 to P_2, and P_2 to D. Each phase may involve a non-polar node. During the first phase, the path of the packet is revealed until P_1. When it reaches P_1, P_1decrypts the first layer of encryption using its private key and reveals the destination address of P_2. Similar process happens at P_2 in order to reveal the destination address of D. However, P_2 does not know whether the next address is the ultimate destination or not, as it has no information that could indicate itself as the second polar node. Therefore, the true destination of the packet is successfully concealed until the destination itself decrypts the third layer of encryption. Thus, cooperation is enforced throughout the packet transmission.

2.3.4.2 COFFEE

The COFFEE protocol [Song & Zhang (2009)] use similar approach as AD-MIX, i.e. by obscuring the ultimate destination of packets, in order to enforce packets forwarding between intermediate nodes. It differs from AD-MIX in the way it transmits packets. Instead of using unicast transmission, it utilizes broadcast transmission in order to transmit packets from source to destination. Due to this feature, it can also hide the next hop of a packet from a receiving node throughout the packet's transmission. When a source node, S wants to send a packet to a destination node, D, COFFEE modifies the path from S to D by adding another intermediate node after D in order to force a loopback to D . The loopback ensures that D is involved in forwarding the packet destined for itself. For instance, if there are intermediate nodes $N_1$and N_2 between S and D, then COFFEE will modify the path from S-N_1-N_2-D to S-N_1-N_2-D-N_4-D .

Consider a case of S sending a packet to D using the path above. A packet in COFFEE protocol consists of a header and a body. The packet body contains the data for D, which S encrypts with a randomly generated key using symmetric encryption, while the header contains the key of the encrypted data, which S encrypts with the public keys of nodes on the path in the order of D-N_4-$D - N_2 - N_1$, and hash of each of the public keys encryption. The header also contains a hash of the randomly generated key. When an intermediate node receives the packet, it first decrypts the packet with its private key and then calculates the hash value of the decryption. If the calculated hash has the same value as the hash of its public key encryption, then it broadcasts the packet to its neighbor without knowing the exact next hop of the packet. On the other hand, if the hash is same as the hash of the randomly generated key, then it is the ultimate destination of the packet. The same process happens at each intermediate node. The ultimate destination is known only after all nodes along the path, except S, have decrypted the packet.

2.4 Analysis of Existing Cooperation Enforcement Models

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

2.4.1 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 using virtual currency 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. However, in credit-based models that use actual currency, the problem can be avoided as the incentive to keep forwarding packets remains especially if forwarding packets are profitable for nodes i.e. the payment exceeds the total cost of forwarding packets [Peirce (2000)].

Third, a common drawback suffered by credit-based models is they do not consider nodes that are located on the outskirts of a network [Huang et al. (2004)]. 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. However, if they are mobile, they can position themselves in the network to earn more credits [Zhang et al. (2007)].

Fourth, some of the existing approaches may have a scalability issue. The Sprite approach [Zhong et al. (2003)], 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. The overhead of storing and processing the receipts, however, can be reduced if each receipt is generated for each forwarding session instead of each message [Mahmoud & Shen (2012, 2013)].

2.4.2 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 [Douceur (2002)].

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. The false detection rate can be reduced by lowering the ratio of decrement to increment of a node's reputation index as a result of its packet forwarding behavior [Refaei et al. (2005)].

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 [Yau & Mitchell (2003)]. 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. This kind of problem can be avoided if the mechanism does not require nodes to exchange reputation information between them [Refaei et al. (2005)].

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. Due to this, other reputation-based approaches prefer isolating selfish nodes so that they can be prevented from using the network.

2.4.3 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 [Yu & Liu (2007)]. 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. As imperfect monitoring could lead to nodes being falsely accused as selfish, one way to mitigate it is to give nodes the chance to recover and not being permanently marked as selfish [Wei & Liu (2008)].

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 [Srinivasan et al. (2003)] 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 [Yu & Liu (2007)], 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.

2.4.4 Analysis of Anonymity-based Models

Anonymity-based models obscure the final destination of packets in order to motivate intermediate nodes to forward packets. The intermediate nodes are prevented from being selfish as there is a possibility that the packets that they need to forward are intended for them. Nevertheless, the models also suffer some drawbacks.

First, the AD-MIX protocol is vulnerable to collusion of polar nodes [Song & Zhang

(2009)]. One way to break the AD-MIX protocol is to let a node knows that it is the second polar [Sundaramurthy & Belding-Royer (2003)]. This can be achieved if two polar nodes collude with each other. When the first polar node decrypts a packet that it receives from a source node, it gets the destination address of the second polar node. The first polar node then can inform the next polar node that it is the second pole. By having this information, the two polar nodes can collude to drop packets that are not intended for them. COFFEE, on the other hand, does not suffer such problem as nodes use broadcast transmission to send or forward packets and they do not know the path of the packets.

Anonymity-based models require the existence of PKI for distribution of nodes' public keys, which are needed for packets encryption. However, as discussed in section 1.2, there is no globally accepted PKI for self-organized MANETs. Therefore, unless the dependency on PKI is removed, anonymity-based models cannot be realized until there is an agreed solution of PKI for MANETs.

2.4.5 Summary

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. Existing credit-based approaches using virtual currency suffers from the problem of excessive credits. By using actual currency, on the other hand, the problem could be prevented. Security module is an essential requirement for credit-based approaches.

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 [Buchegger & Le Boudec (2002)] evaluate the trustworthiness of the second-hand observation. Regarding the reaction to selfish misbehavior, isolation of selfish nodes are 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, have the problem of imperfect monitoring whereby the nodes may acquire the wrong information from the environment. This problem can be mitigated if nodes have the chance of redemption after they have been accused of being selfish. 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.

Anonymity-based approaches are vulnerable to collusion of nodes if the route path of packets transmission is not hidden to nodes. This problem can be mitigated if broadcast transmission is used and intermediate nodes do not know the next hop of a packet. Anonymity-based approaches also rely on encryption in order to enforce cooperation between nodes in MANETs. As a consequence, anonymity-based approaches can only be realized only if there exists a globally accepted PKI for MANETs.

Comparing the existing approaches, credit-based and anonymity-based approaches do not involve monitoring and identity management. However, credit-based approaches require either tamper-proof hardware or central bank to manage payments, and anonymity-based approaches rely on PKI system. Reputation-based and game-based approaches, on the other hand, do not require those credit management elements. However, they have issues on monitoring and identity management. The prerequisite of monitoring and a unique identity linked to the behavior of each node in the network, arise from the requirement of maintaining knowledge of past interactions. For example, in the reputation-based system, the knowledge 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 [Trivers (1971)]. 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

[Alexander (1987)]. 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.

Credit-based and anonymity-based approaches have the advantage of not relying on the maintenance of knowledge of past interactions. However, credit-based approaches require the use of tamper-proof hardware or centralized third-party service while anonymity-based approaches require the existence of PKI system. Reputation-based and game-based approaches, on the other hand, have the advantage of not requiring tamper-proof hardware or centralized third-party service but depend on the maintenance of knowledge of past interactions. Therefore, credit-based and anonymity-based approaches are suitable for use when there is no reciprocity exists. Our work also involve investigating cooperation without reciprocity. We acknowledge the efforts of improving credit-based approaches toward low communication and processing overhead. However, we try to explore a new way of enforcing cooperation in MANETs when there is no reciprocity exists, without having to depend on tamper-proof hardware, centralized third-party service or PKI system.

2.5 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 [Antal et al. (2009); Axelrod et al. (2004); Griffiths & Luck (2010); Hales & Edmonds (2005); Hammond & Axelrod (2006a,b); Ihara (2011); Riolo et al. (2001); Shultz et al. (2008); Spector & Klein (2006); Traulsen & Schuster (2003)]. They, however, only consider stationary environment where nodes have fixed positions such as donation scenario [Riolo et al. (2001)] and peer-to-peer networks (P2P) [Hales & Edmonds (2005)]. 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 2.4.5 as they do not require keeping knowledge 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 [Hales & Edmonds (2005)].

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 [Hales & Edmonds (2005); Spector & Klein (2006)], tag and strategy linkage [Jansen & Baalen (2006)], agents dispersal and cost to benefit ratio [Hammond & Axelrod (2006a)], incomplete social information [Masuda & Ohtsuki (2007)] and space and population structures [Antal et al. (2009); Lehmann & Perrin (2002); Spector & Klein (2006)].

2.5.1 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.

2.5.1.1 Tags

Tags, in the context of tag-based cooperation, are traits, markings or features that are attached to individuals or agents. They can be observed by other agents in order to decide whether to cooperate [Holland (1995)]. 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 [Hales & Edmonds (2005)] or the visible patterns on animals which assist the selective mating process between them [Holland (1995)]. In computational models, these tags can be represented by real numbers [Riolo et al. (2001)] or bit strings [Hales & Edmonds (2005)].

A key property of tags is that they provide a mechanism to structure populations [Holland (1995)]. By using tags, population can be divided into groups with each group formed by agents with similar tags. The mechanism on how tag-based approaches can promote high level of cooperation has been explained in section 2.5.

2.5.1.2 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 change in the population.

2.5.1.3 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.

2.5.2 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.

2.5.2.1 Riolo et al.

Riolo et al. (2001) 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

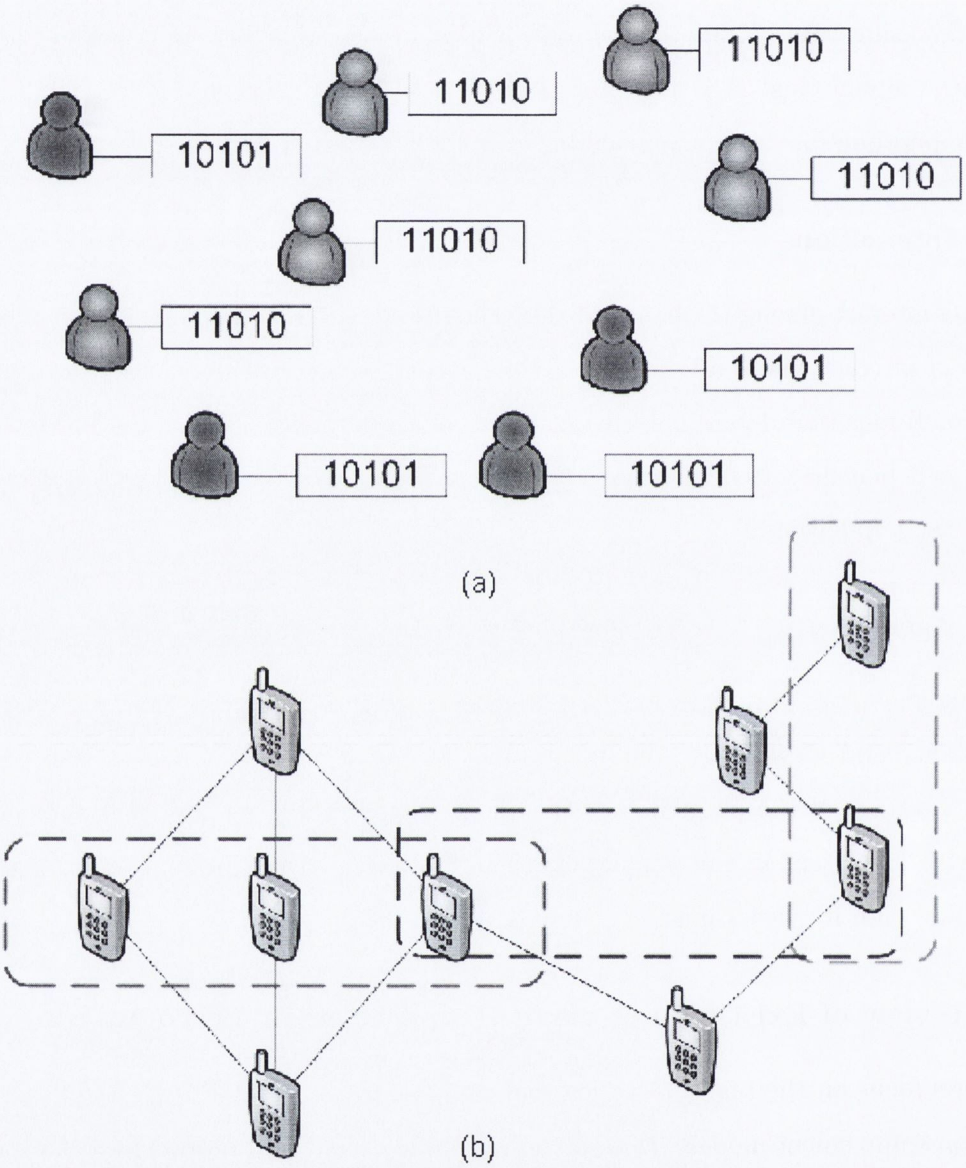

Figure 2.4: Examples of tag: (a) computational model: bit strings as tags; (b) network model: neighbors as tags

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 $|\tau_{\mathrm{A}} - \tau_{\mathrm{B}}| \leq T_{\mathrm{A}}$ 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).

2.5.2.2 Hales and Edmonds

In Hales and Edmonds' approach [Hales & Edmonds (2005)], 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 all of its neighbors, connects to the other node and its neighbors, and copy the other node's strategy. In evolutionary perspective, this process represents the reproduction of agent with better fitness. Figure 2.5(a) and (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.

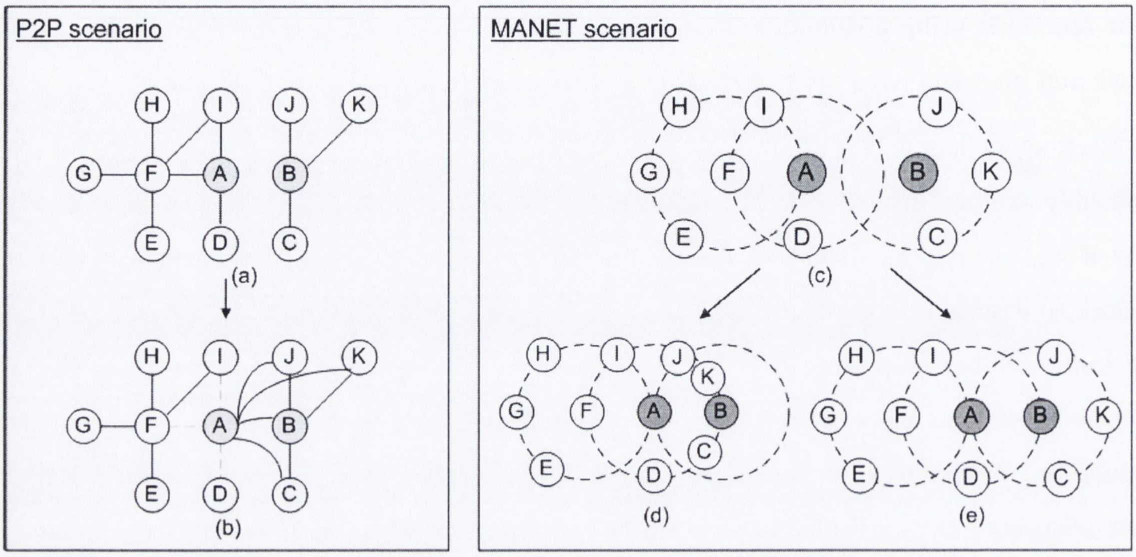

Figure 2.5: Comparison between P2P and MANET scenarios using Hales and Edmond's approach.

2.5.2.3 Griffiths and Luck

Griffiths & Luck (2010) 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 $|\tau_{\mathrm{A}} - \tau_{\mathrm{B}}| \leq T_{\mathrm{A}}$ [Riolo et al. (2001)] to $|\tau_{\mathrm{A}} - \tau_{\mathrm{B}}| \leq (1-\gamma).T_{\mathrm{A}} + \gamma.C_{\mathrm{A}}$ where C_A is the average of context assessment values of agent A's neighbors. 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 modify 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).

2.5.3 Analysis of Existing 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 [Riolo et al. (2001)]; 90% donation rate [Griffiths & Luck (2010)]; and 99% cooperation [Hales & Edmonds (2005)]) there are several issues that need to be discussed.

First, in order to be identified as a tag-based approach, an approach should have three main characteristics which are tags, interactions and agents. For an agent's feature to be selected as a tag, the feature should be able to structure the population into groups. For example, in the reviewed models, the population is partitioned into groups where agents in each group have similar real numbers [Griffiths & Luck (2010); Riolo et al. (2001)] or same list of neighbors [Hales & Edmonds (2005)]. However, in MANETs, using real numbers as tags could not structure the population into groups as nodes with similar number may not necessarily move within each other's transmission range. Using lists of neighbors as tags in mobile environment could also not be able to divide the population into groups as each and every node's neighbors keep changing due to mobility of nodes. Therefore, a suitable feature of mobile nodes that could structure the population, other than what have been proposed in previous models, should be investigated and then selected as a tag.

Second, 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 Figure 2.5(c)), the reproduction process similar to 2.5(a) and (b) could happen only if node B and its neighbor are in node A's transmission range (refer Figure 2.5(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 Figure 2.5(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.

Third, in the model proposed by Riolo et al., agents with similar tags are assumed to help each other. Henrich (2004) 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 & Axelrod (2006a) 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 this traits, there will be agents that receive cooperation from others of the same tag but always defecting. These agents can be classified as selfish.

Fourth, the context assessment proposed by Griffiths and Luck can be viewed as maintaining knowledge of past interactions. As a consequence, it will have the same issues 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 2.4.5.

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

2.6 Summary

This chapter 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. Credit-based models have the advantage of not relying on knowledge of past interactions while reputation-based and game-based approaches have the advantage of not relying on tamper-proof hardware or centralized bank service. Tag-based cooperation enforcement, which has both advantages, 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. Table 2.1 and 2.2 compares the issues, features and management of the existing cooperation enforcement approaches and tag-based approaches, respectively. The following chapters detail the design, implementation, and evaluation of our approach, MaTaCo, a mobility-aware tag-based cooperation enforcement system which takes into account the issues of existing tag-based cooperation enforcement models.

Types	Approach	Management		Features				Issues		
				Payment model		Payment security				
		Centralized	Distributed	Source-based	Destination-based	Local hardware	Credit server	Scalability	Excessive credits	Security module
Credit-based	Anderegg and Eidenbenz	Yes	No	Yes	No	No	Yes	Low	Yes	Yes
	Buttyan and Hubaux	No	Yes	Yes	Yes	Yes	No	High	Yes	Yes
	Yoo et al.	Yes	No	Yes	No	No	Yes	Low	Yes	Yes
	Zhong et al.	Yes	No	Yes	No	No	Yes	Low	Yes	Yes
				Observation		Reaction				
		Centralized	Distributed	First-hand	Second-hand	Avoidance only	Isolation	Unique identity	Prone to false detection	Punish selfish nodes
Reputation-based	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
				Monitoring		Network scenario				
		Centralized	Distributed	Per-node	Per-session	Static ad-hoc network	MANET	Unique identity	Perfect monitoring	Domain knowledge
Game-based	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

Table 2.1: Comparison of the existing cooperation enforcement approaches. The 'Management' column refers to whether an approach is managed by a centralized entity or distributed entities. The 'Features' column summarizes the important characteristics of existing approaches in the context of enforcing cooperation. The 'Issues' column refers to the drawbacks of existing approaches that can affect their performance in enforcing cooperation.

Approach	Management	Features				
		Tags	Interactions	Agents		
				Strategy	Mobile	View range
Riolo et al.	Distributed	Real numbers	Simple donation	Cooperate within group	No	Unlimited
Hales and Edmonds	Distributed	Lists of neighbors	Prisoner's Dilemma/P2P file-sharing	Cooperate within group	No	Unlimited
Griffiths and Luck	Distributed	Real numbers	Simple donation	Cooperate within group	No	Unlimited

Table 2.2: Comparison of the existing tag-based approaches. The 'Management' column refers to whether an approach is managed by a centralized entity or distributed entities. The 'Features' column summarizes the important characteristics of existing approaches in the context of enforcing cooperation, i.e. types of tags and interactions, and agents' attributes. Agents' attributes include their strategy in interacting with other agents, whether they are mobile or not and their view range. Unlimited view range means that agents can interact with any other agent in a population.

Chapter 3

MaTaCo: Mobility-aware Tag-based Cooperation

This chapter describes the Mobility-aware Tag-based Cooperation (MaTaCo) approach to cooperation enforcement in mobile environments or MANETs. The MaTaCo approach models individual nodes in mobile environments or MANETs as adaptive tag-based agents capable of adapting their cooperation to changing mobile environment. In contrast to previous work on tag-based cooperation (refer Section 2.5.2), MaTaCo provides a mobility-aware tag design that incorporates a mobility metric. This allows an agent to measure its tag similarity to its neighbor's based on their relative mobility. Each agent runs the MaTaCo protocol locally which leads to global cooperation enforcement in the network.

The remainder of this chapter is structured as follows: section 3.1 describes a couple of requirements that should be satisfied by an efficient tag-based cooperation enforcement system for mobile environment. Section 3.2 provides the motivations for and an overview of the overall design. Section 3.3 describes the MaTaCo approach and presents the designs of its agent and interaction components. The algorithm used in MaTaCo approach is also described in the section.

3.1 Requirements

As a consequence to the analysis of existing cooperation enforcement models, requirements are identified that serve as guidelines toward the design of our tag-based cooperation enforcement system. An efficient tag-based cooperation enforcement system for mobile environment or MANETs must address the design requirements simultaneously. The identified requirements are as follows:

1. **R1** *Aware of nodes' transmission range limit.* In MANETs, wireless nodes have limited transmission range. This means that a node could only communicate with other nodes that are within its transmission range. In contrast to existing tag-based approaches which assumes a node can communicate with any other nodes in a network, the proposed system should be aware of nodes' transmission range limit. Any process of the system that involves a pair of nodes should only occur if the pair is within each other's transmission range.

2. **R2** *Aware of nodes' mobility.* The mobility of nodes in MANETs creates dynamic environments in which each node's neighborhood changes frequently. In contrast to existing tag-based approaches which are targeted for wired networks in which nodes are stationary, the proposed system should be aware of nodes' mobility. It should be responsive and adaptive to changing mobile environment and unable to dictate nodes' movement simultaneously.

   (a) **R2a** *Respond to changing mobile environment.* The system should respond to changing mobile environment in a network such that it maintains the existence of local interaction groups in the network. This means that in any mobile scenario, each node in the network should be able to determine whether its neighboring nodes are in the same local interaction group as itself.

   (b) **R2b** *Adapt to changing mobile environment.* When the system responds to changing mobile environment, nodes should adapt its behavior according to the response. They should be able to choose the behavior that suits current situation.

(c) **R2c** *Unable to dictate nodes' movement.* The mobility of nodes is a feature of MANETs and its pattern depend on nodes' movement. The nodes themselves decide on how they should move in the network. Their mobility is not a feature of the system. Thus, it should not be able to dictate node's movement.

3. **R3** *Ability to form local interaction groups.* Forming local interaction groups in a network is one of the important aspects of tag-based approaches. Based on the principle of tag-based cooperation, the formation of local interaction groups in the network would guarantee nodes to maximize their payoffs provided that they choose to cooperate in their local interaction groups. While existing tag-based approaches have been able to form local interaction groups in stationary environments, the proposed system should be able to form local interaction groups in mobile environments within the constraints of **R1** and **R2**.

4. **R4** *Execute algorithm at each node independently.* In self-organized MANETs such as civilian MANETs, each node belongs to a different authority and is independent of each other. Therefore, the proposed system should ensure that the algorithm can be run independently at each node. The independent algorithm execution at each node should lead to global cooperation enforcement in the network.

By satisfying these requirements, the system would be able to utilize nodes' mobility and limited transmission range characteristics in order to enforce cooperation in mobile environment or MANETs.

3.2 Overview and Motivations

MaTaCo presents a new approach to the problem of cooperation enforcement in mobile environments or MANETs. It is a tag-based approach that, compared to existing cooperation enforcement models for MANETs, does not require keeping memory of past interactions such as observation logs and reputation records. Hence, it does not need a monitoring mechanism or unique identities that are linked to each observed behavior. A number of tag-based approaches for cooperation enforcement were discussed in section 2.5.2. The approaches have been proved to be capable of promoting high cooperation between agents. However, the approaches are only targeted for stationary agents that have complete view of their environment. Therefore, it is in our interest to investigate how a tag-based approach performs in mobile environments especially MANETs. In contrast to existing tag-based approaches, MaTaCo takes into account the mobility of agents and their limited transmission range. It is targeted for applications whereby agents in the environment are mobile and have incomplete information about the environment. These properties would have an impact on the choice of tags. For instance, in MANETs, using real numbers as tags could not lead to the formation of local interaction groups in the networks as nodes with similar number may not necessarily move within each other's transmission range. Using lists of neighbors as tags in mobile environment would also not be able to structure the population into groups as each node's neighborhood keeps changing due to nodes mobility. Therefore, a suitable feature of mobile nodes that could structure the population, other than what have been proposed in previous models, should be considered as tags.

MaTaCo architecture consists of two main components i.e. agent and interaction. The agent component comprises of tag and strategy while the interaction component defines the scenario that the agents are involved in, the agents' payoff function and the reproduction process of agents. In order to satisfy the requirements, the design of tag in MaTaCo incorporates a mobility metric which was originally proposed for cluster formation in MANETs [Basu et al. (2001)]. This is discussed in more detail in the next section.

3.3 MaTaCo: Mobility-aware Tag-based Cooperation

This section presents MaTaCo approach that satisfies the identified requirements for an efficient tag-based cooperation enforcement system. First, we present the design of agent and interaction components. Then, we describe a distributed tag-based algorithm that utilizes the design of the two components.

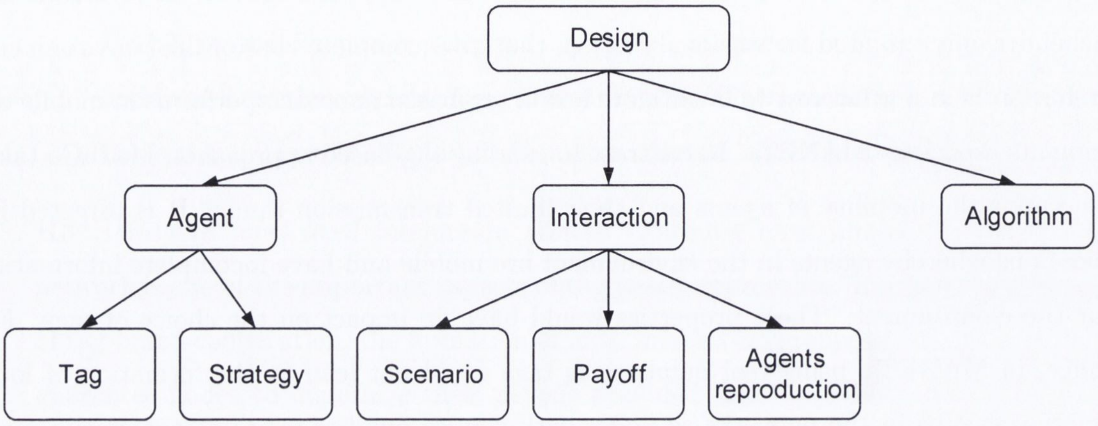

Figure 3.1: Design components of MaTaCo. The components are divided into agent, interaction and algorithm. Agent component is broken down into tag and strategy components while interaction component is broken down into scenario, payoff and agents reproduction components.

3.3.1 Design

This section uses the requirements, *R1*, *R2*, *R3* and *R4* to derive the design of MaTaCo, a mobility-aware tag-based cooperation approach proposed by this thesis. The MaTaCo approach's design is divided into the design of three main components that are complementary i.e. agent, interaction and algorithm components. Figure 3.1 illustrates the design components of MaTaCo.

3.3.1.1 Agent

The design of agent component is further divided into tag and strategy designs which are described in detail in this section.

Tag We recall from section 2.5.1.1 that a tag is an individual trait and observable by others. It should have the ability to structure a population into local interaction groups. For further discussion on the concept of tags, we would like to refer the reader to section 2.5.1.1 and . In our approach, we incorporate the mobility metric proposed by Basu et al. (2001) in the tag design. In their mobility metric, they use the received signal strength which is the power level, $RxPr$, detected at the receiving node as an indicator of the distance between a pair of transmitting and receiving nodes. By using $RxPr$, the relative mobility between a pair of nodes X and Y, $M_Y^{rel}(X)$, is then calculated at the receiving node, Y, as follows:

$$M_Y^{rel}(X) = 10log_{10}\frac{RxPr_{X\rightarrow Y}^{two}}{RxPr_{X\rightarrow Y}^{one}} \tag{3.1}$$

$RxPr_{X\rightarrow Y}^{one}$ is the power level detected at the receiving node Y for the first successive packet transmission from node X while $RxPr_{X\rightarrow Y}^{two}$ is the power level detected at the receiving node Y for the second successive packet transmission from node X. If $RxPr_{X\rightarrow Y}^{two} > RxPr_{X\rightarrow Y}^{one}$, then $M_Y^{rel}(X) > 0$. On the other hand, if $RxPr_{X\rightarrow Y}^{two} < RxPr_{X\rightarrow Y}^{one}$, then $M_Y^{rel}(X) < 0$. A positive value of $M_Y^{rel}(X)$ indicates that the distance between the two nodes is decreasing, meaning the nodes are moving closer to each other while a negative value of $M_Y^{rel}(X)$ means that the distance between the nodes are increasing, indicating that the nodes are moving away from each other. A node with n neighbors would have n values of M^{rel}.

In order to adopt the mobility metric in our tag design, we use the relative mobility, M^{rel} as a node's or an agent's tag. Hence, in our approach, each agent has a dynamic tag that changes as it moves. In our view, the relative mobility between agents is suitable for use as tags in mobile environments. The reason is that it has the ability to structure a mobile population into local interaction groups, e.g. nodes moving closer to each other could form a group and vice versa, which satisfies *R3*. In order to calculate agents' tags, each agent notifies its neighboring agents two times in a time interval. Based on the received notifications, each agent would measure $RxPr^{one}$ and $RxPr^{two}$ for each of its neighbors. The exchange of notifications between two agents is possible only if they are within each other's transmission range, which satisfies *R1*. When an agent X receives $RxPr^{one}$ and $RxPr^{two}$ of another agent, Y, it calculates agent Y's tag using eq. 3.1. The same process happens for each of X's neighbor. Therefore, if X has five neighbors, then it would have a record of five tags, e.g. [+2, +1, -1, +3, -5]. The first value is the tag of its first neighbor, the second value is for its second neighbor and so forth.

Following the approach proposed by Riolo et al. (2001), we also define tolerance threshold. In their approach, a tolerance threshold evaluates whether the tags of two agents are similar or not. Based on their tags similarity, it is determined whether they are in the same local interaction group. From this we can infer that the ultimate purpose of tolerance threshold is to determine whether agents are in the same local interaction group or not. If MaTaCo uses the same equation proposed by Riolo et al. (2001), then MaTaCo would not accurately determine if two agents are in the same local interaction group. This is because the relative mobility between them is used as their tags. For instance, consider a case in which agent X and agent Y are neighbors, both's tags are -1 and the tolerance threshold value is 0. Based on the equation proposed by Riolo et al. (2001), $|\tau_X - \tau_Y| \leq T$, where $\tau_X$is X's tag, τ_Y is Y's tag and T is the tolerance threshold, MaTaCo would decide that the two agents are in the same local interaction group. This is inaccurate as the negative tags indicate that the two agents are moving away from each other and there is a possibility that they are moving to outside each other's transmission range. Therefore it is not suitable for them to be in the same local interaction group. In order to accurately determine if two agents are in the same local interaction group, we use the following equation in which we define the tolerance threshold, $T = 0$. It is worth to note that all agents have the same tolerance threshold value. Therefore, in our approach, X and Y are considered to be in the same local interaction group only if:

$$M_Y^{rel}(X) > T \tag{3.2}$$

Otherwise, they are considered not to be in the same local interaction group. This means that if Y's tag at X is positive, then X determines that Y is in the same local interaction group as itself, otherwise X considers Y not to be in the same group. X also evaluates its other neighbors based on this equation. By incorporating the mobility metric in the design of tag and tolerance threshold, each agent becomes aware of other agents' mobility. Each agent also becomes responsive to changing mobile environment in the way that it can evaluate whether a neighbor is in the same local interaction group as itself based on their relative mobility. Hence, MaTaCo approach satisfies the mobility-aware and responsive features stated in *R2a*.

The motivation of using the mobility metric, i.e. eq. 3.1 and 3.2, as discussed in Basu et al. (2001) are that it does not rely on the availability of location and velocity information (e.g. global positioning system). The mobility metric calculation can be done locally at each agent and the received signal strength can be measured with existing hardware.

Strategy An agent's strategy defines the move or action that it will take when it interacts with another agent. In our approach, an agent can choose between two actions i.e. cooperate or defect as its strategy. Furthermore, an agent's strategy is divided into its strategy with agents that are in the same local interaction group as itself, $S1$ and its strategy with agents that are not in the same group, $S2$. Therefore, in MaTaCo approach, an agent can cooperate (C) or defect (D) with a neighbor that is in the same local interaction group and cooperate or defect with a neighbor that is in different local interaction group.

$$S1 = \{C, D\} \tag{3.3}$$

$$S2 = \{C, D\} \tag{3.4}$$

This design gives each agent the ability to adapt to changing mobile environment. An agent adapts to changing mobile environment in the way that it can choose to play $S1$ or $S2$ with a neighbor based on their relative mobility, hence satisfying the adaptive feature stated in *R2b*. Moreover, it also follows the suggestion by Hammond & Axelrod (2006a) that each agent should possess two traits of strategy i.e., cooperate or defect when interacting with agents that are in the same local interaction group as itself and cooperate or defect when interacting with agents that are not in the same group, in order to avoid the absence of selfish agents in the environment. When each agent possess this traits of strategy, there will be agents that receive cooperation from others of the same tag but always defecting. These agents can be classified as selfish.

3.3.1.2 Interaction

This section describes the interaction component design which is divided into the designs of scenario, payoff and reproduction of agents.

Scenario The scenario dictates what kind of interaction that agents play between them. In this thesis, we propose two models to evaluate our approach which are generic and application-specific respectively. In the generic model, agents play a prisoner's dilemma (PD) game scenario while in the application-specific model, agents plays packets forwarding in MANETs.

The motivation for the choice of PD game as the scenario for the generic model is that it represents the scenario of *forwarder's dilemma* explained in section 1.1.1.1. Similar to *forwarder's dilemma*, in a PD game, agents receive higher scores by defecting than cooperating, independent of their opponent's move. Therefore defection (D) is the dominant strategy in a PD game; assuming that they always try to maximize their payoffs, they would always choose D. However, the dilemma is that if they cooperate with each other, they would receive better payoffs than if they defect. In our work, we assume repeated interactions between two agents are rare because of the mobility of agents. Moreover, tag-based approaches do not rely on history of interactions. Therefore, we choose one-shot PD game as the generic scenario.

The motivation for choosing packets forwarding in MANETs as the scenario for the application-specific model is that a session of packets forwarding, between a source and a destination that are far from each other, would involve multi-hop communication. This would serve as a challenge for MaTaCo in enforcing cooperation between nodes in MANETs, especially in the presence of selfish nodes.

Payoff The payoff function defines the rewards that a pair of agents receive when they play their strategies against each other. The function depends on the scenario that agents are playing. Section 4.3.2.2 and 5.1.2.2 will discuss the payoff functions for PD game scenario and packet forwarding in MANETs and their motivations, respectively.

Reproduction of agents In a tag-based system, it is assumed that agents always try to maximize their payoffs. The reproduction of agents is based on this assumption. For instance, in the approach proposed by Riolo et al. (2001), agents with higher payoffs are reproduced more than agents with lower payoffs. Each reproduced agents inherit the tag and tolerance threshold of its parent. In contrast, we adopt the learning interpretation of reproduction where each agent compares its payoff with another agent's payoff and copies the other's traits such as tag and tolerance threshold if the other agent has higher payoff than its own [Riolo et al. (2001)]. This is similar to Hales and Edmonds' approach. However, instead of copying the tag and strategy, an agent, in our approach, only copies the strategy of the other agent if the other agent's payoffs is higher than its own. We let the tags of agents change according to their movements. The rationale is that if an agent is allowed to copy the tag of a higher scoring agent, then the movements of the agent and its neighborhood need to be controlled so that the agent could have the same $RxPr$ as the higher scoring agent. This is not suitable for mobile environments such as MANETs as each node's movement follows its own trajectory. Therefore, in our work, we let each agent moves according to its own trajectory which satisfies *R2c,* and try to find conditions that promote high cooperation in such a mobile environment.

3.3.1.3 Algorithm

We propose a distributed algorithm that makes use of the design described in section 3.3.1. This section describes the algorithm in general. In the next two chapters, the algorithm is adapted according to the agent-based and MANETs models. The algorithm is designed to run locally at each agent, which satisfies *R4*. This is because in self-organized MANETs, nodes are independent of each other and belong to different authorities. Nevertheless, when all nodes in a network run the algorithm, it should lead to global cooperation enforcement in the network. The algorithm is described in the following steps:

1. Send first notification to neighboring agents.

2. Measure the received power level, $RxPr^{one}$, of each first notification received from neighbors.

3. Send second notification to neighboring agents.

4. Measure the received power level, $RxPr^{two}$, of each second notification received from neighbors.

5. If the second notification of a neighbor is not received within a time interval, discard the neighbor from neighbors list.

6. Calculate M^{rel} for each neighbor.

7. Choose $S1$ if playing with a neighbor with $M^{rel} > 0$, otherwise choose $S2$.

8. Compare payoff with a randomly selected neighbor, j.

9. Copy j's $S1$ and $S2$ if j's payoff is higher than own's payoff.

10. Reset payoff.

11. Repeat from step 1 for next generation.

Step 1 to 5 refers to the process of measuring received power levels of neighboring nodes. Step 6 refers to the process of calculating each neighbor's tag based on the received power levels. Step 7 refers to the process of evaluating whether each neighbor is in the same local interaction group and selecting strategy based on the evaluation. Finally, step 8 to 10 refers to the process of learning interpretation of agents reproduction as described in section 3.3.1.2. Figure 3.2 shows the flow of the algorithm.

3.4 Design Analysis

In order for a tag-based approach to successfully enforce cooperation between agents in a population, it must be able to divide the population into local interaction groups. This is because only with the existence of local interaction groups in the population, do the agents have the incentives to cooperate in order to maximize their payoffs (as discussed in section 2.5). Existing tag-based approaches, such as Griffiths & Luck (2010), Hales & Edmonds (2005) and Riolo et al. (2001), are successful in enforcing high level of cooperation in populations of stationary agents as they have the ability to divide the populations into local interaction groups. In the approaches, each agent could identify agents that share the same group as itself from the entire population. In MANETs, however, there is a possibility that the existing approaches could not enforce high level of cooperation as MANETs environment is different in the sense that nodes are mobile and have limited transmission range. Their mechanisms are not aware of nodes' mobility and nodes' limited transmission range would only allow them

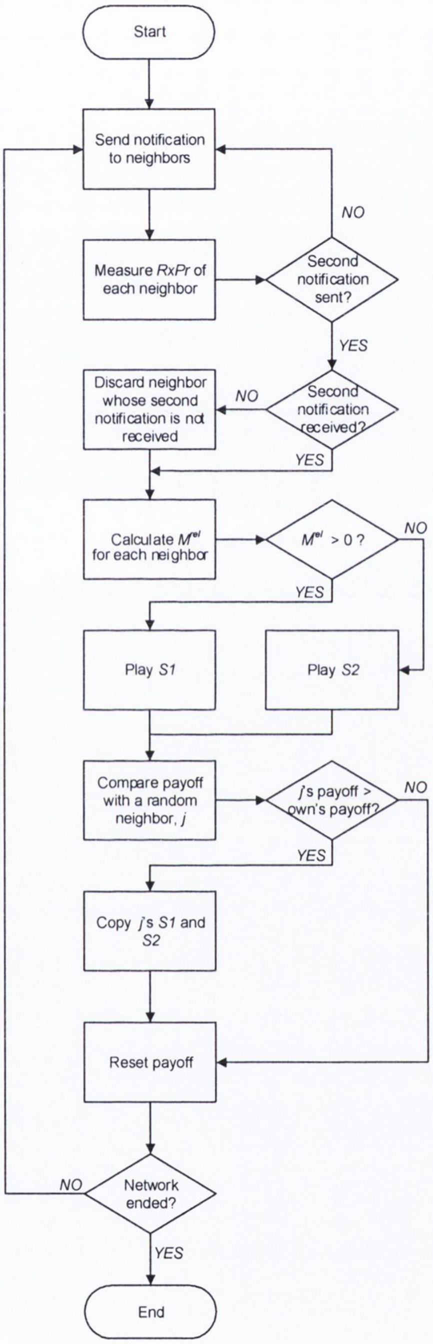
Start
Send notification to neighbors
Measure RxPr of each neighbor
Second notification sent?
NO
YES
Second notification received?
NO
Discard neighbor whose second notification is not received
YES
Calculate M^rel for each neighbor
M^rel > 0 ?
NO
YES
Play S1
Play S2
Compare payoff with a random neighbor, j
j's payoff > own's payoff?
NO
YES
Copy j's S1 and S2
Reset payoff
Network ended?
NO
YES
End

Figure 3.2: MaTaCo's algorithm flow chart. $RxPr$ refers to the received power level of the received notification. M^{rel} is the relative mobility between a pair of nodes. A node with n neighbors has n values of M^{rel}. $S1$ and $S2$ are the strategies of a node.

to locate group members from their neighborhoods, not the entire network. Therefore, the challenge of a tag-based cooperation enforcement approach, in mobile environment especially MANETs, is to be able to form local interaction groups with the constraints of nodes' mobility and limited transmission range.

Distinct from existing approaches, MaTaCo is designed to have the ability to divide populations of mobile nodes, especially MANETs, into local interaction groups while simultaneously aware of nodes' mobility and limited transmission range. By using relative mobility between nodes as tags, nodes that run MaTaCo algorithm should be able to form local interaction groups in a MANET based on their mobility. Moreover, each node only has to identify its group members from its neighborhood instead of the entire network, thus adhering to its limited transmission range. To be more specific, a node would only form a local interaction group with its neighbors that are moving closer to itself. They are identified based on their tags, i.e. positive tags mean that they are approaching while negative tags mean that they are moving away. Based on the principle of tag-based cooperation, a node should be cooperative in its local interaction group in order to maximize its payoff. Thus in this sense, the solution amounts to the enforcement of cooperation between nodes that are approaching each other. This solution is expected to solve the problem of selfishness in MANETs as it adheres to the principle of tag-based cooperation and the constraints of MANETs. In tag-based cooperation, local interaction groups have to be formed in order to ensure nodes prefer to be cooperative rather than selfish while in MANETs, a node can communicate directly only with other nodes that are within its transmission range. Therefore, in MANETs, a local interaction group can only be formed between nodes that are within each other's transmission range.

With regards to the proposed solution, nodes that are approaching each other, in a MANET, form a local interaction group within their transmission range. If they choose to be cooperative in the group, then they create a cooperative region in the network. Nodes in the cooperative region will gain higher average payoffs compared to a group of nodes that forms a selfish region. Assuming all nodes always try to maximize their own payoffs, the selfish nodes will copy the cooperative nodes' behavior when they find out that the cooperative nodes are gaining higher payoffs than themselves. Subsequently, majority of nodes in the network will be cooperative. If majority of nodes in the network are cooperative, then any pair of source and destination nodes, that are not within each other's transmission range, will have a high probability of being able to find a cooperative multi-hop route through the network [Hales & Edmonds (2005)]. This also justifies why the solution targets the enforcement of cooperation with nodes that are approaching rather than those receiving.

3.5 Summary

This chapter presented the MaTaCo approach, a mobility-aware tag-based cooperation enforcement approach in which the enforcement of cooperation takes into account the mobility and transmission range characteristics of wireless agents. Four main requirements for MaTaCo were identified as a consequence to the analysis of existing cooperation enforcement approaches, i.e. aware of nodes' mobility (*R1*), aware of nodes' transmission range (*R2*), ability to form local interaction groups (*R3*) and execute algorithm at each node independently (*R4*). In order to satisfy *R1*, *R2* and *R3*, MaTaCo incorporates a mobility metric in its mechanism. The mobility metric utilizes relative mobility between nodes as tags which gives MaTaCo the ability to form local interaction groups in mobile environment especially MANETs. With the formation of local interaction groups in MANETs, cooperation between nodes can be enforced based on the principle of tag-based cooperation. *R4* is satisfied by ensuring MaTaCo's algorithm can be run locally at each node without any collaboration. Analysis of MaTaCo's design was also presented in order to justify why MaTaCo is expected to solve the problem of selfishness in MANETs. The next chapter describes MaTaCo's implementation and evaluation in an abstract, mobile environment model. Chapter 5 describes the implementation and evaluation of MaTaCo in a MANET model. Its results in both chapters are compared to the performances of existing tag-based models reviewed in Chapter 2.

Chapter 4

TACME: Tag-based Cooperation in Mobile Environment

Building on a review of cooperation enforcement in MANETs and tag-based cooperation literature in chapter 2, chapter 3 outlined a mobility-aware tag-based cooperation enforcement approach that could be used to enforce cooperation in mobile environments. The approach was designed to incorporate agents' mobility and transmission range characteristics in the tag-based mechanism. This chapter will follow on from this by describing the process of building a generic model to test and evaluate the proposed approach outlined in chapter 3. The generic model is an agent-based model. Therefore, this chapter will begin by introducing agent-based modeling and describing the tools that can be used to develop agent-based models in section 4.1 and 4.2 respectively. Section 4.3 explains the design of TACME with respect to the MaTaCo design. Section 4.3 describes the agent-based model developed to evaluate the modified MaTaCo approach. The evaluation of the modified MaTaCo approach in the agent-based model is presented and discussed in section 4.4.

4.1 Agent-based Modeling

Agent-based modeling is a method of modeling systems that comprise autonomous entities called agents that can interact between them and with their environment. Each agent has the ability to decide its future action locally based on a set of interaction rules [Bonabeau (2002)]. Moreover an agent in an agent-based model is able to make local decisions without any centralized mechanism [Macal & North (2005)] and respond to changes in its environment with a goal-directed response[Wooldridge & Jennings (1995)]. In our view, with these characteristics of an agent, agent-based modeling is suitable for modeling cooperation between mobile agents in a decentralized system. In such a system, where there is no authority, each mobile agent should be autonomous in deciding whether it should cooperate with other agents or not. Moreover, each mobile agent has to be responsive to changing mobile environment and as its goal is to maximize its own payoff, its response should increase its payoff.

Agent-based modeling can be used in different research areas. For instance, it has been applied to investigate petrol station prices [Heppenstall et al. (2005)], land-use and land-cover change [Parker et al. (2003)], insect population [Parry et al. (2006)], human pedestrian movement patterns [Turner & Penn (2002)], human immune systems [Jacob et al. (2004)] and computer-aided driving [Miller et al. (2003)].

4.2 Tools for Developing Agent-based Models

Tools that are available for agent-based models development include, but are not limited to, Ascape [Parker (2001); Inchiosa & Parker (2002)], MASON [Luke et al. (2005)], Swarm [Minar et al. (1996)] and Repast [North et al. (2007)].

As this thesis involves developing an agent-based model and a network model that are related to each other, the tools for developing both models should be selected by considering that they would not complicate the transition from agent-based model to network model. One way to ensure this is to use the same programming language in both tools. At this point, we have decided that we will be using Java-based JiST/SWANS to implement and simulate the network model. Therefore, based on this, we have to use a agent-based modeling tool that is also Java-based. Ascape, MASON and Repast are Java-based while Swarm has Java-based and Objective-C versions.

One of the main aspects of our simulation is the mobility of agents. In our simulation, agents will be moving based on random waypoint mobility. However, random waypoint mobility (RWM) model and all other mobility models are not available in agent-based modeling tools. Therefore, we have to implement RWM model in the selected agent-based modeling tool. All four tools mentioned above were being considered as they are Java-based. They were evaluated in terms of how feasible it is to implement random waypoint mobility model in each of them. Based on our investigation, we found that Repast Simphony requires the least effort to implement random waypoint mobility model, compared to the other three. The architecture of Repast Simphony allows the agents' mobility to be managed at environment level instead of agent level. This means that we can easily implement an RWM model that conforms to the RWM model implemented in JiST/SWANS and let the simulation environment manage the agents' movement based on the inputs fed into the RWM model. The architectures of the other environments, on the other hand, only allow agent movement to be managed at agent level. This means that for each simulation run, we have to manually input a set of location points for each agent and during the simulation, each agent would need to refer to the set in order to move. Although the location points could be generated from external random waypoint mobility generator such as BonnMotion [Aschenbruck et al. (2010)], we would have to do this everytime before we run a simulation. Based on this, we determined that selecting Repast Simphony would be the most appropriate choice of the reviewed environments. Therefore, Repast Simphony will be used for the development of the abstract model described in this chapter.

4.3 Design of TACME

We develop an agent-based model, TACME, to study how the proposed tag-based mechanism performs in a mobile environment. TACME is a generic model in which agents interact without MANET protocol. Thus, this model provides an ideal, error-free environment for evaluating the performance of MaTaCo approach. The idea is to ensure that our approach works as expected before moving on to implementing it in a mobile network simulator; which will introduce additional factors that may influence the functionality of our approach. If we would implement the proposed approach in a mobile network simulator without first evaluating it in agent-based model and then find out that the approach is not working as expected, it would be difficult to determine the cause of the problem; whether the approach just simply would not work or it is affected by MANET protocol. By first implementing our approach in TACME, at least we would know whether it works as expected or not, without involving MANET protocol. This section describes the design of TACME model in three parts i.e. agent, interaction and algorithm.

4.3.1 Agent

Agents in TACME model are mobile agents that employ modified MaTaCo mechanism. The MaTaCo approach was modified to use distances between agents for measuring tags similarity, instead of using received power levels, $RxPr$ as in the original MaTaCo approach.This section describes the agent component design in three parts i.e. tag, strategy and mobility.

4.3.1.1 Tag

Instead of using the received power, $RxPr$ (discussed in section 3.3.1.1), we use the real distances between transmitting and receiving agents to calculate agents' tags in TACME model. This is because TACME model only captures the mobility of nodes and not the networking part of MANETs. Moreover, TACME model assumes an ideal, error-free environment and the simulator (which will be discussed in section 4.4.1.6) knows the physical location of all agents. Therefore, we use Friis' free space transmission formula Friis (1946) to derive the relationship between the received power, $RxPr$ and the distance between transmitting and receiving agents, d as follows:

$$RxPr\alpha\frac{1}{d^2} \tag{4.1}$$

and

$$\frac{RxPr^{two}}{RxPr^{one}}\alpha\frac{d_{one}^2}{d_{two}^2} \tag{4.2}$$

where:

- d^2_{one} =distance between transmitting and receiving agents for the first successive transmission, and

- d^2_{two} =distance between transmitting and receiving agents for the second successive transmission.

Based on this, we modify eq. 3.1 as follows:

$$M_Y^{rel}(X) = 10log_{10}\frac{d^2_{one_{X\to Y}}}{d^2_{two_{X\to Y}}} \tag{4.3}$$

Hence, two agents X and Y are considered to be in the same local interaction group if eq. 4.3 satisfies eq. 3.2. Note that the mechanism of exchanging tags between agents is the same as described in section 3.3.1.1. However, instead of recording $RxPr^{one}$and $RxPr^{two}$, in TACME model, an agent records d^2_{one} and d^2_{two} of its neighbors.

4.3.1.2 Strategy

Each agent in TACME model has two traits of strategy, $S1$ and $S2$ as described in section 3.3.1.1.

4.3.1.3 Mobility

The movement of agents in TACME model is based on random waypoint mobility (RWM) model. RWM model is one of the most widely used mobility models in MANET simulation [Camp et al. (2002)]. In this mobility model, each node selects a random destination within the simulation area and a speed v from an input range $[v_{min},v_{max}]$ where v_{min} is the minimum speed allowed for the mobile node and v_{max} is the maximum allowable speed. The node then moves towards the destination at its selected speed. Once it reaches the destination, it stays for a predefined pause time. At the end of the pause time, it selects another destination and speed and resumes movement. The process is repeated until the end of simulation time.

4.3.2 Interaction

This section describes the design of interaction component of TACME model in three parts i.e. scenario, payoff and reproduction of agents.

4.3.2.1 Scenario

In TACME model, agents play prisoner's dilemma (PD) game with each other. The rationale behind the choice of PD game as the scenario is that PD game captures the situation of *forwarder's dilemma* explained in section 1.1.1.1. Similar to *forwarder's dilemma*, in a PD game, an agent always gets a higher score by defecting than cooperating, independent of its opponent's move. Therefore defection (D) is the dominant strategy; assuming that agents are rational in the sense that they are always trying to maximize their payoff, both agent would always choose D. However, the dilemma is that if they cooperate with each other, their payoff would be better than if they both defect. Thus, it is in our interest to evaluate whether the MaTaCo mechanism can enforce the agents to resist the defection and choose to cooperate in a mobile environment. Note that a rational agent is an agent that has the ability to determine how to achieve its preferred outcomes, given the actions of other agents Osborne & Rubinstein (1997).

PD game can be classified as one-shot or iterated PD (IPD) game. In IPD game, a pair of agents play more than one round of PD game with each other. Agents are assumed to recognize each other and remember their history of interactions. In our work, we assume repeated interactions between two agents are rare because of the mobility of agents. Moreover, tag-based mechanisms do not rely on history of interactions. Therefore, instead of using IPD game, we choose one-shot PD game as the abstract scenario.

4.3.2.2 Payoff

The payoff is defined according to the Prisoner's Dilemma game. In Prisoner's dilemma game, both players or agents receive a reward payoff, R for mutual cooperation and a punishment payoff, P for mutual defection. However, when an agent plays different move than its opponent, the defector receives a temptation to defect payoff, T and the cooperator receives a sucker payoff, S. The payoffs must comply to these two rules; the payoffs ranking T > R > P > S and the restriction 2R > T + S.

4.3.2.3 Reproduction of Agents

The reproduction of agents in TACME model follows the learning interpretation of reproduction described in section 3.3.1.2.

4.3.3 Algorithm

We adapt the algorithm described in section 3.3.1.3 to apply the design of TACME model. The adapted algorithm is described in the following steps:

1. Send first location coordinate to neighboring agents.
2. Measure the distance, d^2_{one}, of each neighbor based on the received first coordinates.
3. Send second coordinate to neighboring agents.
4. Measure the distance, d^2_{two}, of each neighbor based on the received second coordinates.
5. If the second coordinate of a neighbor is not received within a time interval, discard the neighbor from neighbors list.
6. Calculate M^{rel} for each neighbor.
7. Choose an opponent, i, randomly from the neighbor list
8. Play PD game with the opponent; choose $S1$ if playing with a neighbor with $M^{rel} > 0$, otherwise choose $S2$.
9. Calculate payoff.
10. Compare payoff with a randomly selected neighbor, j.
11. Copy j's $S1$ and $S2$ if j's payoff is higher than own's payoff.
12. Reset payoff.
13. Repeat from step 1 for next generation.

4.4 Evaluation

This section details the evaluation of our mobility-aware tag based approach to enforcement of cooperation in mobile environment by means of simulation. First it describes the experimental setup used to conduct the evaluation. Then the rest of this section focuses on the experiments used for the evaluation, as well as their analysis and outcomes.

4.4.1 Experimental Setup

In this section, we first describe the TACME model in order to show what happens during the simulation. We then present the evaluation objective and the baselines used for comparison. The metrics used to measure the performance of our proposed approach in terms of average cooperation rate and average defection rate are also presented. We then discuss on generating mobility patterns for the simulation before moving on to a description of the software, hardware and general parameters used for the simulation.

4.4.1.1 Description of TACME

The TACME model is composed of a set of N agents that have limited view radius and move according to random waypoint mobility model. Limited view radius is a representation of limited transmission range of a node in MANET. Each agent has a set of n neighbors that are moving within its view radius. For instance, agent A becomes agent B's neighbor only if it is moving within agent B's view radius. If agent A then moves away and exit agent B's view radius, then agent A is no longer a neighbor of agent B. The relationship between agent A and B is bidirectional, meaning that if A is B's neighbor, then B is also A's neighbor and vice versa. Furthermore, each agent has two strategy bits. One bit indicates whether it will cooperate or defect with agents that possess similar tag, $S1$ and another one indicates whether it will cooperate or defect with agents that have different tags than itself, $S2$. Both the neighbor list and the strategy bits are only known to itself.

Periodically, each agent sends its first location coordinate to its neighbors and calculates the first distances between itself and its neighbors. Then, each agent sends a second, updated coordinate and calculates the updated distances. After that, each agent choose a neighbor randomly from its list of neighbors. They play a one-shot PD game between them. If they have similar tags, both of them play $S1$. Otherwise, both play $S2$. Each agent receives payoff after playing a game. Then, each agent selects a random neighbor from its list to compare payoffs between them. If the selected neighbor has a higher payoff, then the agent copies the neighbor's $S1$ and $S2$. Otherwise, the selected neighbor copies the agent's $S1$ and $S2$. If their payoffs are the same, then nothing is copied.

4.4.1.2 Evaluation Objective

Chapter 2 outlined the issue with existing tag-based cooperation enforcement models. Riolo et al.'s [Riolo et al. (2001)] (RCA), Hales and Edmonds' [Hales & Edmonds (2005)] (HE) and Griffith and Luck's [Griffiths & Luck (2010)] (GL) models only investigate tag-based cooperation in stationary environments in which agents are not moving physically and have unlimited view radius which makes them able to interact with any other agent in the population. Furthermore, RCA and GL assume that agents with similar tags always help each other. Hence, there is no presence of selfish agents in the model. In addition, GL has similar problems as existing reputation-based cooperation enforcement systems. The context assessment used in GL can be viewed as maintaining knowledge of past interactions. As a consequence, it will have the same issues as existing reputation-based systems such as requiring monitoring of agents and a unique identity linked to the behavior of each agent, as discussed in section 2.4.5. Chapter 3 described the design of MaTaCo, a tag-based cooperation enforcement approach designed to take into account the mobility and limited view radius of agents, while at the same time, does not assume that tags similarity between agents guarantees cooperation between them. The previous sections discuss how MaTaCo approach is adapted in order to fit into TACME, a mobile environment model. This section provides the evaluation of the modified MaTaCo approach in order to assess to which degree requirements are met when it is applied in a generic, mobile environment model.

The following evaluation objective is used:

- *Obj*1: The modified MaTaCo for TACME promotes higher cooperation than RCA and HE in mobile environment under varying conditions, such as initial number of selfish agents, speed of agents, population size and population density.

Based on *Obj*1, we aim to determine the modified MaTaCo's ability to successfully enforce cooperation between mobile agents, in terms of increasing both percentage of conditional cooperators and average cooperation rate in mobile environment. We also aim to determine the limitations of the modified MaTaCo in terms of its ability to adapt to varying conditions mentioned above. The next section presents the baselines used to compare with the modified MaTaCo in order to assess its performance.

4.4.1.3 Baselines for Comparison

We compare the modified MaTaCo against three baselines:

- **No tag**: this baseline allows agents in TACME to interact with each other without employing any tag-based mechanism. Therefore, for this baseline, agents just play PD game with their neighbors in mobile environment. The performance of this baseline justifies whether a cooperation enforcement system is really needed or not. Good performance of this baseline indicates that mobile agents can cooperate with each other without any cooperation enforcement system, and vice versa.

- **RCA**: RCA is implemented as described in section 2.5.2.1 except that interactions between agents are contained within their neighborhood in order to take into account limited view radius of each agent. In the original approach, agents can interact with any other agents from the population. The significance of having RCA as one of the baselines is that we can evaluate whether using real numbers as tags is enough to enforce cooperation in mobile environment.

- **HE**: HE is implemented as explained in section 2.5.2.2. However, similar to RCA, limited view radius characteristic of each agent is taken into account. For similar reason as RCA, by having HE as one of the baselines, we can determine whether using lists of neighbors as tags can enforce cooperation between mobile agents.

We exclude GL from the baselines because of its similar characteristic to existing reputation-based approach which makes it possess similar problems as them (discussed in section 3.3.1.1).

The next section presents the metrics used to assess the performance of modified MaTaCo against *Obj*1.

4.4.1.4 Performance Metrics

We use two metrics to assess the performance of the modified MaTaCo against the baselines outlined before.

- **Percentage of conditional cooperators**: the percentage of conditional cooperators is the percentage of agents that cooperates with other agents that have similar tags and choose to defect when playing against agents with different tags. It indicates whether agents discriminate when cooperating. Cooperation enforcement aims at increasing the percentage.

- **Cooperation rate**: for a given agent, the cooperation rate is the number of times that an agent cooperates over the number of times that the agent plays PD game. It indicates the probability of an agent cooperates when interacting with other agents. Cooperation enforcement aims at increasing the rate.

As the simulation involves many agents, we use a collective metric which is the average cooperation rate (ACR) per agent. The percentage of conditional cooperators in the population at a given time is also used to monitor the ongoing performance. Better performance in terms of the metrics outlined is critical to a tag-based cooperation enforcement approach. The metrics represent the degree to which the main goal of increasing cooperation is met.

The cooperation rate metric is commonly used in tag-based cooperation domain [Griffiths & Luck (2010); Hales & Edmonds (2005); Riolo et al. (2001)]. It is also known as donation rate [Griffiths & Luck (2010); Riolo et al. (2001)]. High cooperation rate indicates that an agent is likely to cooperate when it interacts with other agents. Collectively, this leads to a cooperative environment. Low cooperation rate, on the other hand, indicates that an agent is prone to be selfish. Therefore it is important for an approach to be able to increase the rate. The percentage of conditional cooperators, in our view, is an important metric for evaluating a tag-based cooperation approach. This is because of its relation to the principle

Parameter	Value Format	Description
Population size	Unsigned integer	Defines the total number of agents involved in simulation
Minimum speed	Floating point	Defines the minimum speed allowed, in meters per second, for a mobile agent
Maximum speed	Floating point	Defines the maximum speed allowed, in meters per second, for a mobile agent
Pause time	Floating point	Defines the length of time, in seconds, for which agents should pause before changing direction
Simulation time	Floating point	Defines the duration of simulation, in seconds, in which agents are allowed to move
Area width	Floating point	Defines the width of simulation area, in meters
Area length	Floating point	Defines the length of simulation area, in meters

Table 4.1: The RWM model is ported from a mobile network simulator, JiST/SWANS. Given a set of parameters which defines the population size, minimum and maximum allowable speeds, pause time, area size and simulation duration, it will output commands that dictate agents movement. The simulation environment of Repast Simphony utilizes the commands in order to manage agents movement during simulation runs.

of tag-based cooperation (discussed in section 2.5). Based on the principle, the existence of conditional cooperators or agents that cooperate discriminately based on their tags would lead to a cooperative population. Therefore high percentage of conditional cooperators can be expected to lead to a highly cooperative population. Hence it is crucial for a tag-based approach to have the ability to increase the percentage.

4.4.1.5 Mobility Pattern Generation

As discussed in section 4.2, we use Repast Simphony to develop TACME as the tool's architecture allows us to easily implement mobility model in it. Since both Repast Simphony and JiST/SWANS, the mobile network simulator are Java-based, we reuse the source codes and libraries for the RWM model from JiST/SWANS and port them into Repast Simphony. The source codes and libraries can be downloaded from JiST/SWANS website [Barr (2005)] We then set the simulation environment to manage agents movement based on the mobility patterns generated from the RWM model. A set of parameters required to generate the mobility patterns are illustrated in table 4.1.

RWM model was selected as the mobility model in our evaluation in order to make the evaluation as generic as possible. In our view, other mobility models are very specific to their targeted applications. For instance, although Self-similar Least Action Walk (SLAW) mobility model [Lee et al. (2009)] emulates realistic human mobility, it only represents the mobility patterns of people in a community such as visitors in a theme park and students in university campus. Therefore, our position is that RWM model is the best choice in terms of representing generic mobility patterns. Note that the mobility model only represents the movement of agents. It is not a feature that is embedded into the proposed approach.

4.4.1.6 Simulation Hardware and Software

The evaluation environment consisted of the implementation of the modified MaTaCo approach within the Repast Simphony simulator. Repast Simphony 2.0 package for Windows was used. A machine with Intel Core 2 Duo processor with a clock speed of 2.4 GHz and 3 GB of memory was utilized. Windows XP SP2 was installed on the machine. The Eclipse Compiler for Java (ECJ) in Eclipse SDK version 3.6.1 with Java Runtime Environment (JRE) version 1.6.0.22 was utilized by Repast Simphony.

The simulator is based on the assumption of an ideal environment and does not include the simulation of refractions of signals on obstacles or the absorbing of signals by bodies. This means that the information fed into the approaches is based on an ideal environment and may differ significantly from the real world; however, it is suitable as a basis for a comparison of the approaches against each other.

4.4.1.7 Experimental Parameters

The general parameters, listed in table 4.2, were used in the simulation, unless specified otherwise. The values of the parameters were chosen such that they emulate a scenario of civilian MANET. The values of population size, area size and view radius follow the suggestion by Buchegger & Le Boudec (2002). Therefore the justification for the choices is similar to what have been discussed by them. 50 agents were placed in an area of 1000m by 1000m. This represents the center of a city at a time when it is not busy. Each agent has a view radius of 250m which conforms to the radio range value of an off-the-shelf wireless card [Buchegger & Le Boudec (2002)]. All agents move according to the RWM model with speeds uniformly distributed from 0m/s to 10m/s and each has a pause time of 30 seconds. The speed represents a range of users that are staying at fixed locations, walking, cycling and also

Parameter	Value
Population size	50 agents
Minimum speed	0m/s
Maximum speed	10m/s
Pause time	30s
Simulation time	1100s
Area width	1000m
Area length	1000m
View radius	250m
Interaction starts at	100s
Interaction stops at	1000s
Conditional cooperators	50%
Unconditional defectors	50%
Payoff	$T = 1.9$, $R = 1$, $P = 0.0001$ and $S = 0$

Table 4.2: General parameters of the simulation. All experiments used the values stated in this table, unless specified otherwise.

driving slowly while the pause time represents users that are stopping at certain locations such as a pedestrian who is stopping at a shop for a quick buy or a car driver who is stopping at a junction. We used the values suggested by Hales & Edmonds (2005) to define PD payoffs where $T = 1.9$, $R = 1$, and $P = 0.0001$. However, instead of using $S = P$, we define $S = 0$ to enforce $T > R > P > S$. This is to ensure the payoffs comply to the rules of a PD game, as discussed in section 4.3.2.2.

Each simulation ran for 1100 seconds of simulated time. Interactions between agents started at 100 seconds and ended at 1000 seconds. Therefore, interactions between agents lasted for 900 seconds in each simulation. The chosen simulation and interaction time give agents adequate time to potentially travel the whole simulation area and interact and compare their payoffs between them, respectively. In addition, the first and last 100 seconds of the simulation gave agents time to move to random positions before starting to interact and prevented the interactions from sudden halt due to the end of the simulation respectively. The population started with 50 percent conditional cooperators and 50 percent unconditional defectors. This is to ensure that there is no bias towards either cooperative environment or selfish environment at the start of simulation. A conditional cooperator has $S1 = C$ and $S2 = D$, meaning that it only cooperates with agents that have similar tags. An unconditional defector or selfish agent, on the other hand, has $S1 = D$ and $S2 = D$. The results were averaged over ten runs, each with a different seed. The seed value influences the placement and movement of agents in the simulation.

4.4.2 Experiments

In order to evaluate the performance of the modified MaTaCo in TACME, a series of experiments were conducted employing the Repast Simphony simulator [North et al. (2007)]. The experiments are designed to test the hypothesis that the modified MaTaCo for TACME promotes higher cooperation than RCA and HE in mobile environment under varying conditions, such as initial number of selfish agents, speed of agents, population size and population density. There are two important aspects in the hypothesis that need to be tested i.e. cooperation and robustness. Thus, in the experiments, we measure cooperation rate and percentage of conditional cooperators in order to present the term "cooperation" in quantifiable forms and we test the robustness of the approaches against varying factors by having different categories of experiments. In this section, the experiments are presented and their results are discussed.

4.4.2.1 Experiment 1: Performance over Time

This experiment evaluates the performance of the modified MaTaCo in comparison to the baselines described before, over time. Figure 4.1 and 4.2 show the average cooperation rate and the percentage of conditional cooperators, respectively, over time for the modified MaTaCo, No-tag, RCA and HE.

We observe that if mobile agents play one-shot PD games without tag mechanism, as in No-tag case, the average cooperation rate and the percentage of conditional cooperators decrease to zero over time. This justifies the need of a cooperation enforcement system such as a tag-based system to promote cooperation.

Existing tag-based models such as RCA and HE are not capable of promoting cooperation between mobile agents, as shown in the figures. The results indicate that they could only delay

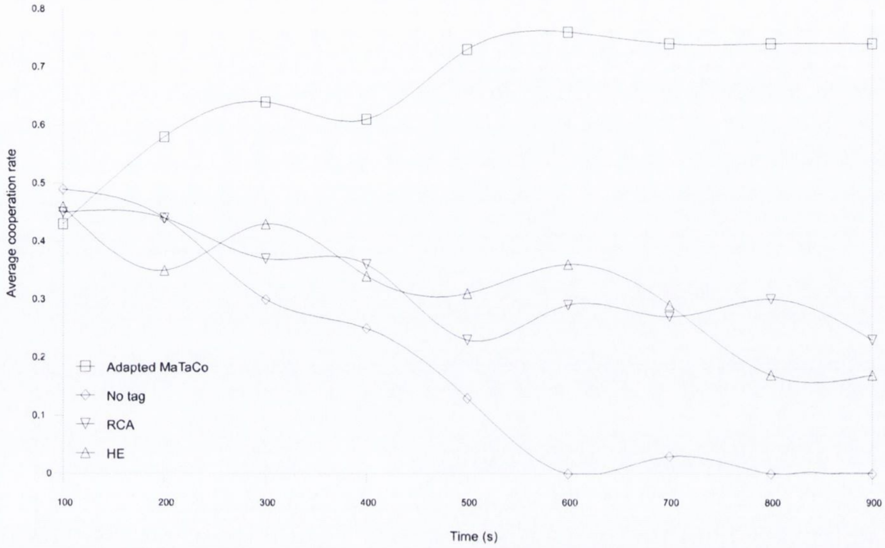

Figure 4.1: Average cooperation rate over time

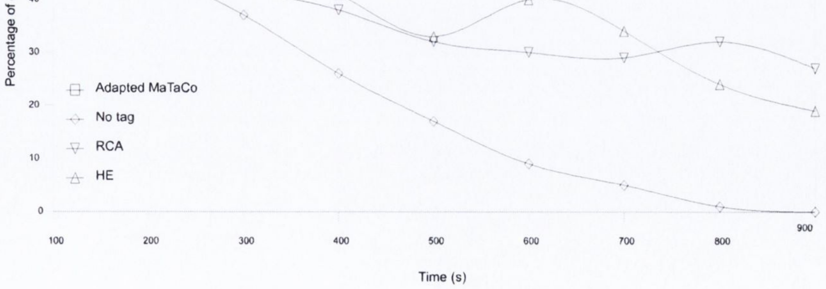

Figure 4.2: Percentage of conditional cooperators over time

the population from reaching total defection. The modified MaTaCo, however, increases the average cooperation rate and the percentage of conditional cooperators over time. Conditional cooperators increases from 50% at the start of simulation to 80% at the end of simulation, while the average cooperation rate rises from 0.44 to 0.73. This shows that the modified MaTaCo is capable of promoting cooperation between agents in mobile environment. The reason it performs better than RCA and HE is that it takes into account the mobility of agents in enforcing cooperation, thus makes it responsive and adaptive to changing mobile environment. RCA and HE, on the other hand, were not targeting to enforce cooperation in mobile environment.

4.4.2.2 Experiment 2: Impact of Mobility

This experiment evaluates the impact of varying agents' speeds on the performance of the modified MaTaCo in comparison to the baselines. Table 4.3 lists the maximum speed settings used in four scenarios. In scenario 1, the speed is uniformly distributed between 0 to 5m/s which represents a range of users that are staying at fixed locations, walking or cycling. In scenario 2, the speed is uniformly distributed between 0 to 10m/s which represents a range of users that are staying at fixed locations, walking, cycling or driving at maximum 36km/h. In scenario 3, the speed is uniformly distributed between 0 to 15m/s which represents a range of users that are staying at fixed locations, walking, cycling or driving at maximum 54km/h. Finally in scenario 4, the speed is uniformly distributed between 0 to 20m/s which represents a range of users that are staying at fixed locations, walking, cycling or driving at maximum 72km/h.

Scenario	Maximum speed (m/s)
1	5
2	10
3	15
4	20

Table 4.3: Maximum speed setting

The average cooperation rate, and the percentage of conditional cooperators at the end of simulation of the modified MaTaCo are compared with the implementation of No-tag, RCA

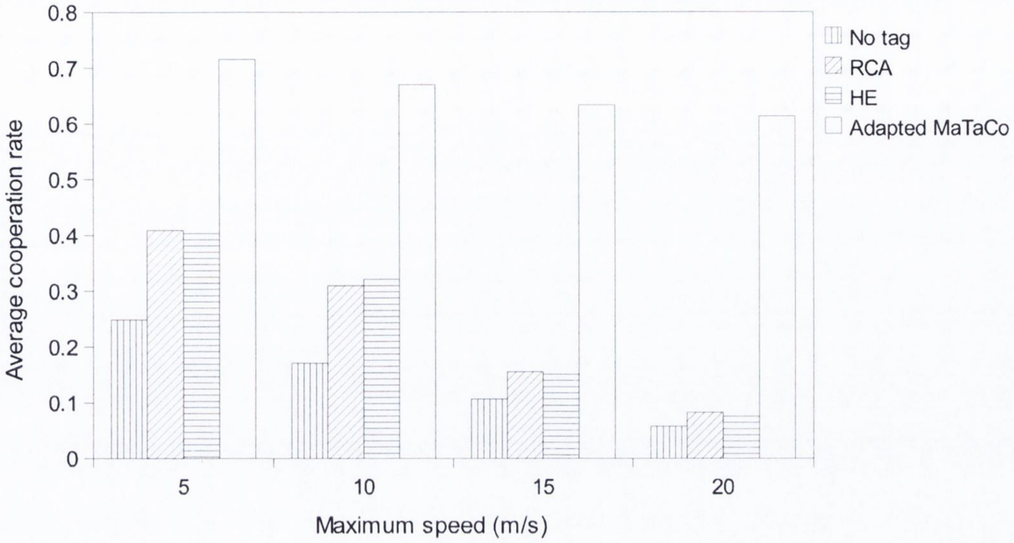

Figure 4.3: Average cooperation rate with respect to agents' maximum speed

and HE. It is expected that the modified MaTaCo will achieve higher average cooperation rate and percentage of conditional cooperators, as it takes into account agents' mobility in enforcing cooperation. Figure 4.3 illustrates the average cooperation rate achieved for a maximum speed of 5 m/s, 10 m/s, 15 m/s, and 20 m/s for the modified MaTaCo, No-tag, RCA and HE. It shows that the modified MaTaCo achieves a higher average cooperation rate than the baselines. As maximum speed increases, the average cooperation rate of the modified MaTaCo drops slightly. This is due to the increase in variation of agents' speeds which decreases the probability of finding agents with similar tags. However, the modified MaTaCo still perform very well compared to the baselines.

Figure 4.4 shows the percentage of conditional cooperators at the end of simulation. As mentioned in section 4.4.1.7, the population starts with 50% selfish agents and 50% conditional cooperators. Therefore, at the end of simulation, the modified MaTaCo increases the percentage of conditional cooperators in the population by 24 to 37% depending on the maximum speed setting. No-tag, RCA and HE, on the other hand, decrease the percentage of conditional cooperators in the population in each of the maximum speed setting. This is expected as the approaches were not designed for mobile environment.

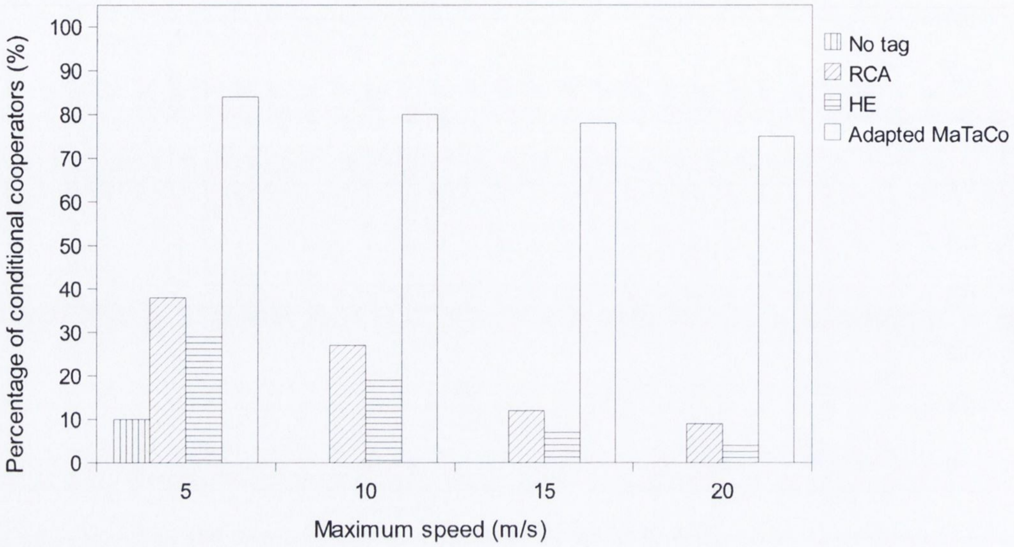

Figure 4.4: Percentage of conditional cooperators at the end of simulation with respect to agents' maximum speed

The results also show that even in low mobility environment i.e. 5 m/s maximum speed, No-tag, RCA and HE are not capable of increasing the percentage of conditional cooperators in the population. The modified MaTaCo, on the other hand, increases the percentage even in high mobility environment i.e. 20 m/s maximum speed. Therefore, we expect that the modified MaTaCo will outperform No-tag, RCA and HE in all scenarios described in the next sections as the scenarios are fixed at 10 m/s maximum speed.

4.4.2.3 Experiment 3: Impact of Selfish Agents

This experiment evaluates the modified MaTaCo's performance in comparison to the baselines, under varying number of selfish agents at the start of simulation. Table 4.4 lists the settings used for selfish agents percentage at the start of population in four scenarios. Figure 4.5 and 4.6 illustrate the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for a percentage of selfish agents of 10%, 20%, 30%, and 40%. As discussed in section 4.4.1.7, starting the simulation with 50% selfish agents and 50% conditional cooperators ensures that there is no bias towards either cooperative or selfish

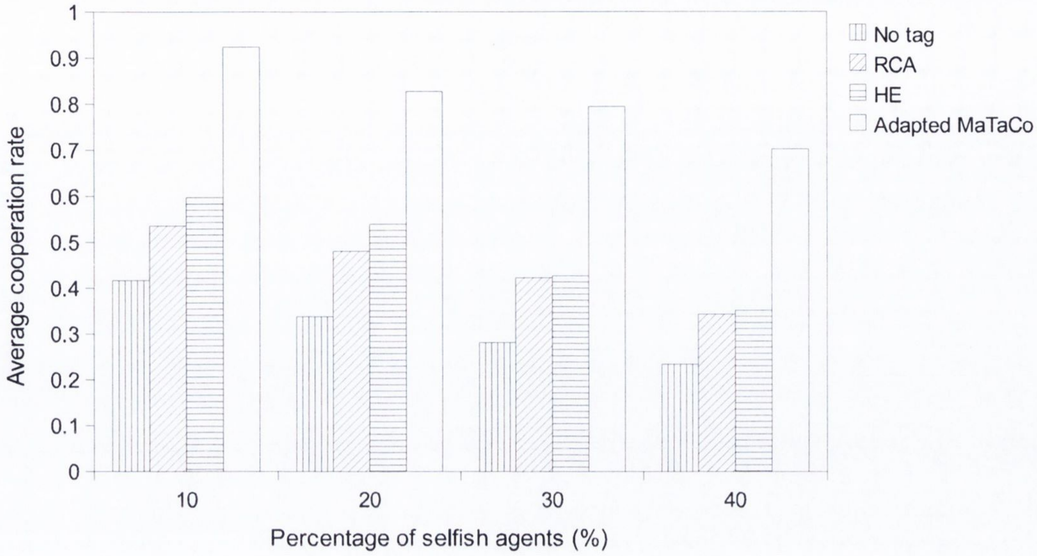

Figure 4.5: Average cooperation rate with respect to percentage of selfish agents at the start of simulation

environment. However, as shown in experiment 4.4.2.1, the baselines do not perform well in that scenario. Intuitively, a higher percentage of selfish agents than 50% at the start of simulation would further degrade the baselines' performance. Therefore, in this experiment, we chose the values ranging from 10% to 40% selfish agents in order to provide a bias towards cooperative environment and evaluate whether it will have any effect on the baselines and also our approach.

Scenario	Selfish agents (% of population)
1	10
2	20
3	30
4	40

Table 4.4: Percentage of selfish agents setting

Both figures show that the baselines do not promote higher cooperation even when there is only 10% selfish agents at the start of simulation. The average cooperation rate and the percentage of conditional cooperators increase only if agents employ the modified MaTaCo. With an increasing percentage of selfish agents, both the average cooperation rate and the

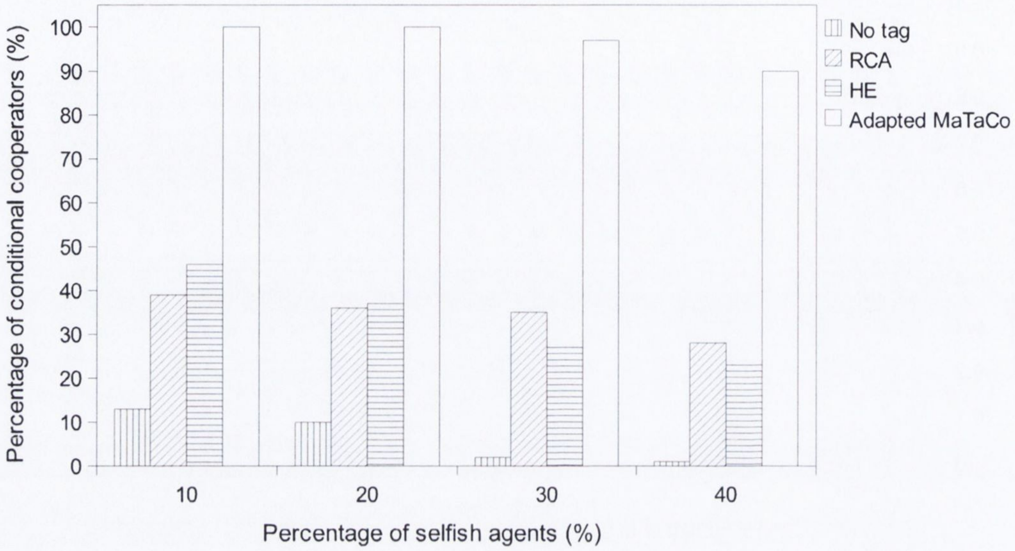

Figure 4.6: Percentage of conditional cooperators at the end of simulation with respect to percentage of selfish agents at the start of simulation

percentage of conditional cooperators decrease. The average cooperation rate has a higher decrease rate than the percentage of conditional cooperators due to low cooperation rate at the early of simulation. With respect to the modified MaTaCo, the percentage of conditional cooperators can reach 100% in 900 seconds if the population starts with 10% or 20% selfish agents. This shows that the modified MaTaCo has the capability to enforce full cooperation in a population of mobile agents. The higher the percentage of selfish agents at the start of population, the longer the time is needed for the modified MaTaCo to enforce full cooperation.

4.4.2.4 Experiment 4: Impact of Population Size

This experiment evaluates the impact of total number of agents on the average cooperation rate and the percentage of conditional cooperators. Table 4.5 lists the population size and corresponding area size settings used in four scenarios. Figure 4.7 and 4.8 show the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for a population size of 100, 200, 300, and 400 agents. The simulation area size is changed accordingly to keep the population density fixed at 20000m^2/agent (which is

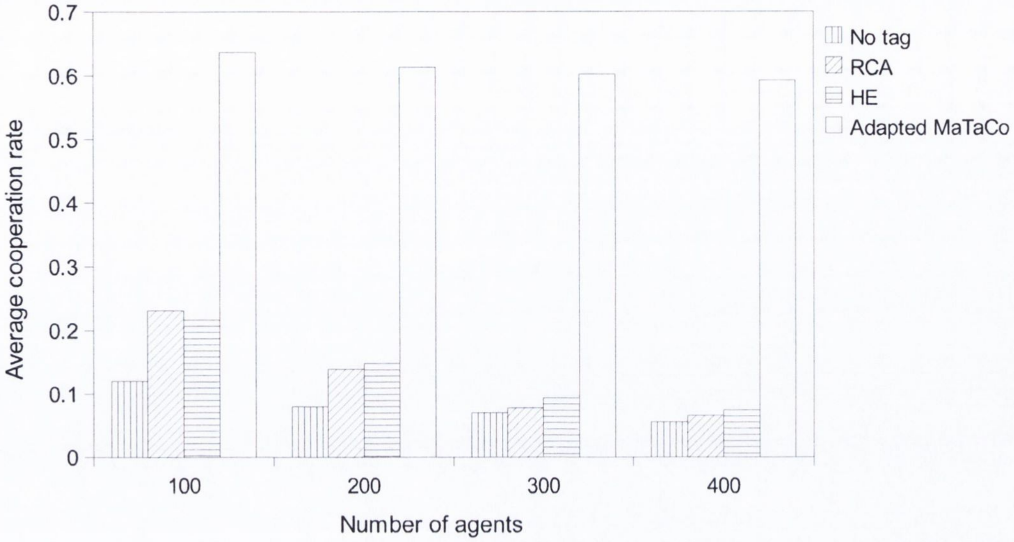

Figure 4.7: Average cooperation rate with respect to number of agents

as same as the population density for 50 nodes in an 1000m x 1000m area). For instance, a population of 400 agents with a density of 20000m^2/agent requires an area of 8000000m^2 which equals to approximately 2828m by 2828m square area. The aim of this experiment is to evaluate the approaches in large population. However, due to limitations of the machine used in terms of its processing capacity, this experiment could only support up to a maximum of 400 agents without consuming more time than was available.

Scenario	Population size	Area size (m x m)
1	100	1414m x 1414m
2	200	2000m x 2000m
3	300	2449m x 2449m
4	400	2828m x 2828m

Table 4.5: Parameter setting

It is observed that in each population size, the modified MaTaCo increases the percentage of conditional cooperators. Hence, the average cooperation rate of the population increases. Both the average cooperation rate and the conditional cooperators percentage of the modified MaTaCo do not decrease significantly as the population grows. This is because of the fact that the maximum speed is fixed at 10 m/s in each case, thus the probability of an agent

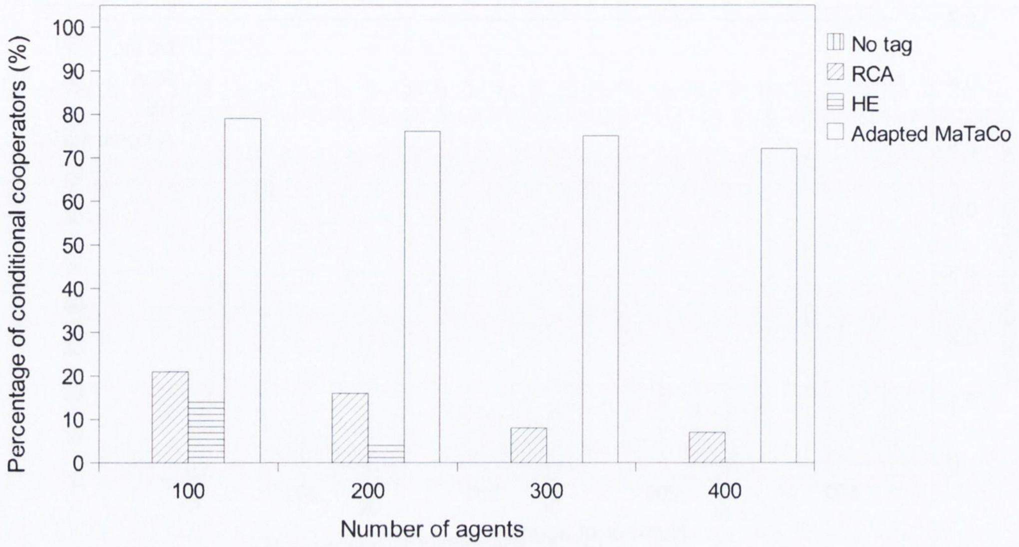

Figure 4.8: Percentage of conditional cooperators at the end of simulation

finding other agents with similar tags does not change significantly between the cases.

4.4.2.5 Experiment 5: Impact of Population Density

This experiment evaluates the average cooperation rate and the percentage of conditional cooperators, when population density varies. Table 4.6 lists the population density and corresponding area size settings used in four scenarios.

Scenario	Population density (m^2/agent)	Area size (m x m)
1	10000	707m x 707m
2	20000	1000m x 1000m
3	30000	1225m x 1225m
4	40000	1414m x 1414m

Table 4.6: Population density setting

Figure 4.9 and 4.10 show the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for a population density of 10000, 20000, 30000, and 40000 m^2/agent. The values were chosen such that they do not exceed the view area of an agent. The view area is defined by πr^2 where r is the agent's view radius. As

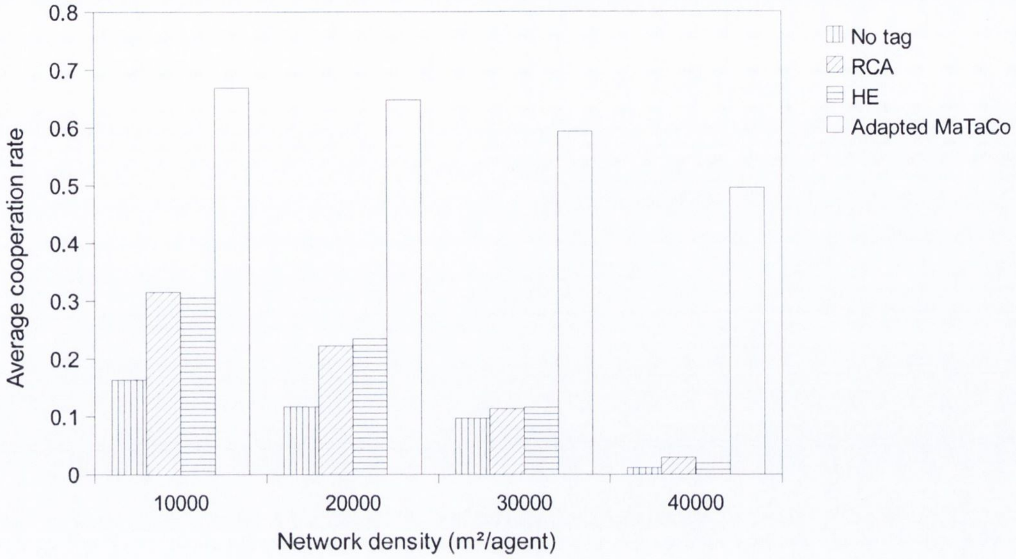

Figure 4.9: Average cooperation rate with respect to population density

each agent's view radius is defined as 250m throughout the simulation, therefore the view area of each agent is approximately 196350m^2 of circle area which is always larger than the chosen population density values. This is important in order to keep the degree of population partitioning as low as possible, so that it would not affect the evaluation. The simulation area size is changed accordingly to keep the population size fixed at 50 agents. For instance, a population of 50 agents with a density of 10000m^2/agent requires an area of 500000m^2 which equals to approximately 707m by 707m square area.

It is observed that both the rate and the percentage decrease as network density decreases. This is due to the fact that each agent's view radius is limited to 250 m. Thus, as the area size increases which in turn decreases the network density, the probability of an agent finding neighbors decreases as each agent has a larger area to move around. With a decreasing probability of an agent finding neighbors, the probabilities of an agent finding other agents with similar tags and an agent has a neighbor to compare its payoff with also decrease.

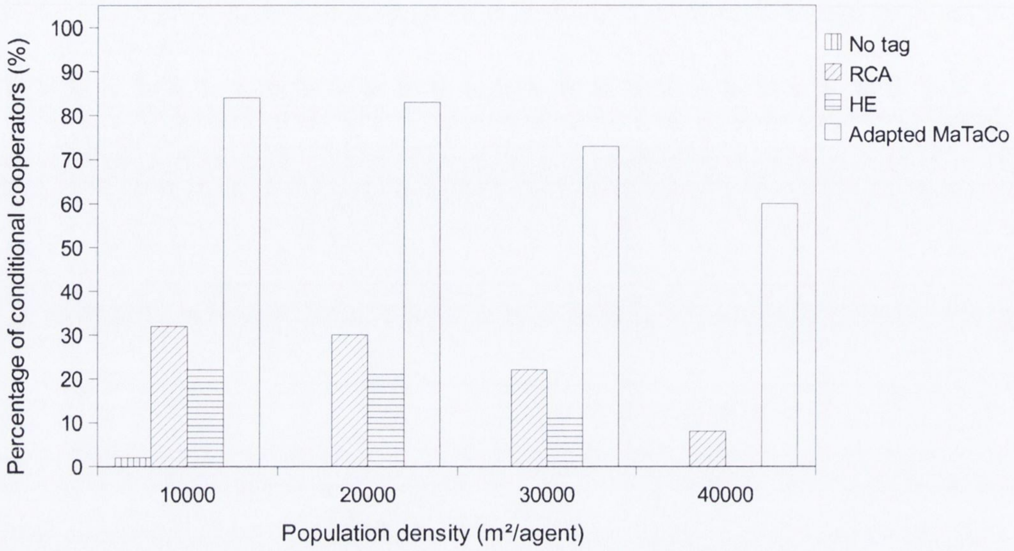

Figure 4.10: Percentage of conditional cooperators at the end of simulation with respect to population density

4.5 Summary

This chapter described the development of TACME, a mobile environment model for tag-based cooperation. The agent-based modeling technique and tool used for TACME development were discussed. In this model, there was no radio communication involved. Therefore, the MaTaCo approach was adapted to use distances between agents for measuring tags similarity, instead of using received power levels, $RxPr$ as in the original MaTaCo approach. The relationship between the distance between two agents and the received power level was derived from Friis' free space transmission formula. Agents in TACME played PD games between them as TACME generalized a packet forwarding session in a MANET as a PD game.

This chapter also presented the evaluation of the modified MaTaCo in TACME, in comparison to the No-tag, RCA and HE approaches. A set of experiments that assess the performance of the modified MaTaCo in terms of promoting higher cooperation than the baselines under varying conditions, was outlined. Overall, the modified MaTaCo outperformed the baselines under all tested conditions. The modified MaTaCo increased the average cooperation rate and the percentage of conditional cooperators under varying number of selfish agents, speed of agents, population size and population density. The baselines, on the other hand, decreased the rate and the percentage under the varying conditions.

In the next chapter, we present the development of TACMAN, a MANET model for tag-based cooperation and evaluates MaTaCo and the baselines in TACMAN. We expect that MaTaCo and the baselines in TACMAN perform similarly to the modified MaTaCo and the baselines in TACME.

Chapter 5

TACMAN: Tag-based Cooperation in Mobile Ad hoc Networks

The development of TACME, an agent-based model for evaluating tag-based cooperation in mobile environment was presented in chapter 4. This chapter outlines the development of TACMAN, a MANET model for evaluating the MaTaCo approach outlined in chapter 3. Section 5.1 outlines the design of TACMAN with respect to the MaTaCo design. Section 5.2.1.1 provides a detailed description of TACMAN. The evaluation of MaTaCo approach performance in TACMAN is presented and discussed in section 5.2.

5.1 Design of TACMAN

In addition to the TACME model, we develop a MANET model called TACMAN to study the performance of MaTaCo approach in a mobile ad hoc network environment. In this model, agents are mobile nodes that communicate with each other wirelessly using MANET protocols. This section presents the design of TACMAN model in three parts i.e. agent, interaction and algorithm.

5.1.1 Agent

Agents in TACMAN model are mobile nodes that employ MaTaCo mechanism. This section describes the agent component design in three parts i.e. tag, strategy and mobility.

5.1.1.1 Tag

In TACMAN model, $RxPr$ is used as the basis of a node's tag. Therefore, its design is as described in section 3.3.1.1.

5.1.1.2 Strategy

Each agent in TACMAN model has two traits of strategy, $S1$ and $S2$ as described in section 3.3.1.1. In packet forwarding game in MANETs, forwarding a packet is a form of cooperation while discarding it is a form of defection. Therefore, in this model, we adapt eq. 3.3 and eq. 3.4 as follows:

$$S1 = \{F, D\} \tag{5.1}$$

$$S2 = \{F, D\} \tag{5.2}$$

where F and D refer to forward and discard actions.

5.1.1.3 Mobility

In order to provide the same mobile environment as in the TACME model, TACMAN uses RWM model as the mobility model (refer section 4.3.1.3).

5.1.2 Interaction

In this model, interactions between nodes are performed using wireless communication based on MANET protocols. This section describes the design of interaction component of TACMAN model in three parts i.e. scenario, payoff and reproduction of agents.

5.1.2.1 Scenario

In this model, nodes interact with each other in packet forwarding games. In a packet forwarding game, a packet is relayed from a source node to a destination node through intermediate nodes. The packet forwarding game ends if the destination node receives the packet or one of intermediate node drops or discards it. The action of an intermediate node is defined by its strategy as mention in section 5.1.1.2. In our work, we assume that a node selects its forwarding strategy based on the tag of preceding node. Consider a packet forwarding game which involves a source node S, three forwarding nodes $F1$ and $F2$, and a destination node D. If node S sends a packet to $F1$, then $F1$ selects its forwarding strategy, whether $S1$ or $S2$, based on the similarity between $F1$'s and S's tags. Then, if $F1$ forwards the packet and $F2$ receives it, $F2$ will decide its strategy based on the similarity between $F2$'s and $F1$'s tags, not between its tag and$S$'s tag. Hence, tag-based interactions are contained within a node's neighborhood. After the game has ended, each intermediate node receives its payoff based on its action in the game.

5.1.2.2 Payoff

In TACMAN model, the payoff of a node in a time period, P, is defined as follows:

$$P = b - c \tag{5.3}$$

where:

- $b =$ the ratio of the total number of its packets delivered to the total number of packets it generated, in that time period, and
- $c =$ the ratio of the total number of others' packets it forwarded to the total number of forwarding requests it received in that time period.

The rationale behind this equation is that it captures the *forwarder's dilemma* as described in section 1.1.1.1. The variable b can be seen as benefits of using the network where a node use other nodes' services to get its packets delivered to intended destinations. The variable

c, on the other hand, can be seen as costs of using the network where a node has to provide its service for others' benefits. Therefore, a selfish node would avoid from forwarding others' packets in order to maximize its payoff. The dilemma is that if all nodes in a network behave selfishly, then each node would have a zero payoff. If that is the case, they would all be better off if they cooperates with each other.

5.1.2.3 Reproduction of Agents

The reproduction of agents in TACMAN model follows the learning interpretation of reproduction described in section 3.3.1.2.

5.1.3 Algorithm

We adapt the algorithm described in section 3.3.1.3 to apply the design of TACMAN model. The adapted algorithm is described in the following steps:

1. Broadcast first hello message to neighboring nodes.
2. Measure the power level, $RxPr^{one}$, of each first hello message received from neighbors.
3. Broadcast second hello message to neighboring nodes.
4. Measure the power level, $RxPr^{two}$, of each second hello message received from neighbors.
5. If the second hello message of a neighbor is not received within a time interval, discard the neighbor from neighbors list.
6. Calculate M^{rel} for each neighbor.
7. Play packet forwarding game with randomly selected neighbors.
8. Choose $S1$ if receiving a packet that needs to be forwarded from a neighbor with $M^{rel} > 0$, otherwise choose $S2$.
9. Calculate payoff.
10. Compare payoff with a randomly selected neighbor, j.

11. Copy j's $S1$ and $S2$ if j's payoff is higher than own's payoff.

12. Reset payoff.

13. Repeat from step 1 for next generation.

5.2 Evaluation

This section presents an evaluation of our mobility-aware tag based approach to cooperation enforcement in a MANET by means of simulation. Our simulations are based on a network simulator, Java in Simulation Time/Scalable Wireless Ad hoc Network Simulator (JiST/SWANS) [Barr et al. (2005a,b)]. This section first discusses the experimental setup for evaluating MaTaCo. Then it details the experiments used for the evaluation and presents their analysis and outcomes.

5.2.1 Experimental Setup

This section first describes the simulation scenario of TACMAN model. It then presents the objective of evaluation, baselines and performance metrics used to assess MaTaCo's performance. It also discusses mobility pattern generation, software, hardware and parameters for the simulation.

5.2.1.1 Description of TACMAN

The TACMAN model is composed of a set of N nodes that have limited transmission range and move according to random waypoint mobility model. Each node has a set of n neighbors that are moving within its transmission range. Furthermore, each node has two strategy bits. One bit indicates whether it will forward or discard packets received from neighbors that have similar tags, $S1$ and another one indicates whether it will forward or discard packets received from neighbors that have different tags than itself, $S2$. Both the neighbor list and the strategy bits are only known to itself.

Periodically, each node sends its first hello message to its neighbors and calculates the received power levels of each first hello message received from its neighbors. Then, each node sends second hello message and calculates the received power levels of each second hello message received. From the measured first and second received power levels, each node calculates the relative mobility for each of its neighbors. Then, each node plays packet forwarding game with randomly chosen neighbors. If it is selected as an intermediate node in the game and receives a packet that needs to be forwarded from a neighbor that has similar tag, then it plays $S1$. Otherwise, it plays $S2$. After the packet forwarding game ended, each node involved in the game calculates its payoff. Then, each node selects a random neighbor from its list to compare payoffs between them. If the selected neighbor has a higher payoff, then the node copies the neighbor's $S1$ and $S2$. Otherwise, the selected neighbor copies the node's $S1$ and $S2$. If their payoffs are the same, then they keep their own strategy.

Selfish Nodes In TACMAN, we modeled selfish nodes according to the first category of selfish nodes defined by Michiardi & Molva (2002b). As described in section 1.2, selfish nodes in this category participate in the network routing and maintenance but refuse to contribute to the data packet forwarding.

Combining with Routing Protocol We used a reactive routing protocol called Ad hoc On-Demand Distance Vector (AODV) [Perkins & Royer (1999)] as the routing protocol in the simulations. In AODV, a source node broadcasts a route request (RREQ) whenever it wants to find a route to a destination node. Any intermediate node may reply to the request by sending a route reply (RREP) if it receives the request and has a route to the destination node. Otherwise, it rebroadcasts the RREQ. When the destination node receives the request, it unicasts a RREP back to the source, along the reverse route. Upon receiving the route reply, the source node starts sending data packets to the destination node. If an intermediate node detects a link break in an active route, it sends a route error message (RRER) to the source node through the active reverse route. In AODV, connectivity between neighboring nodes may be maintained by broadcasting control messages. If a node has not broadcasted a control message within a time interval, then it broadcasts a hello message to its one-hop neighbors. On the other hand, if a node has not received a hello message from its neighbor within a specified number of time intervals, then the connection to the neighbor has failed.

Combined with MaTaCo, a node, i, needs to measure the $RxPr^{one}$ of a neighbor node, j, if i receives a RREQ from j and j is not in i's neighbors list. In order to maintain connectivity with i, j should broadcast a hello message periodically, within *ALLOWED_ HELLO_ LOSS * HELLO_ INTERVAL* from the last message, e.g. RREQ or hello message, broadcasted. *ALLOWED_ HELLO_ LOSS* is the maximum number of periods of *HELLO_ INTERVAL* a node should wait before confirming a link to a neighbor is lost. We used the recommended values for *ALLOWED_ HELLO_ LOSS* and *HELLO_ INTERVAL* which are two and one second respectively [Chakeres & Royer (2002)]. Therefore, j should broadcast a hello message within two seconds from the last message it broadcasted. Upon receiving the hello message broadcasted from j within two seconds after it receives the RREQ from j, i measures the $RxPr^{two}$ of j. If i did not receive a hello message from j within the specified time, then i removes j from its neighbors list. This means that j would also detect a loss of connectivity to i.

After a route from a source node to a destination node is established through a number of intermediate nodes and each intermediate node has calculated the M^{rel} of preceding node, the source node starts sending data packets to the destination node. For each data packet received by the destination node, it sends an acknowledgment message (ACK) to the source node along the active reverse route. The source node then calculates its payoff based on the ACKs received. For each ACK received, the source node increases the number of its packets delivered by one. A source node should receive an ACK within a timeout interval specified by *ACTIVE_ ROUTE_ TIMEOUT*. We used a default value of three seconds for the parameter. Therefore, if a source node did not receive an ACK within three seconds after it has forwarded a data packet, the packet is considered not delivered. An intermediate node does not have to know the behavior of other intermediate nodes in the same route. This is because each node calculates its payoff using eq. 5.3 independent of other nodes' behaviors. For each packet an intermediate node forwarded, it increases its number of others' packets forwarded by one.

Each node should wait until an active route, that it is involved in, timed out before comparing its payoff with other node. In order to compare payoff, each node broadcasts a hello message that contains its payoff and strategy. If a node finds a higher payoff, it copies the strategy linked to the payoff. Otherwise, its strategy remains the same.

5.2.1.2 Evaluation Objective

The previous chapter evaluated the modified MaTaCo approach in mobile environment. The MaTaCo approach was modified in the way that a tag of agent X at agent Y refers to the square of the distance between X and Y. In this chapter, we use the MaTaCo approach as described in 3. We only modify the notification mechanism so that it would fit into a MANET protocol and keep the design of tag and tolerance. Therefore, this section presents the evaluation of MaTaCo in a MANET. The evaluation assesses to which degree the goals of enforcing cooperation and reducing defection are met when MaTaCo is applied in a MANET.

The following objective of evaluation are used:

- $Obj1$: MaTaCo promotes higher cooperation than RCA and HE in MANETs under varying conditions, such as initial number of selfish nodes, speeds of nodes, network size, network density and network load.

Based on $Obj1$, we intend to evaluate MaTaCo's ability to successfully enforce cooperation between mobile nodes in a MANET, in terms of increasing percentage of conditional cooperators, average cooperation rate and packet delivery ratio of the network. We also intend to evaluate MaTaCo's limitations in terms of its ability to adapt to varying network conditions mentioned above. The next two sections discuss the baselines and performance metrics used to assess MaTaCo against $Obj1$, respectively.

5.2.1.3 Baselines for Comparison

We compare MaTaCo against three baselines i.e. no tag, RCA and HE, and exclude GL for the same reason, as described in section 4.4.1.3.

5.2.1.4 Performance Metrics

We use three metrics to evaluate MaTaCo's performance against the baselines.

- **Cooperation rate**: for a given node, the cooperation rate is the ratio of the number of times that the node forwards a packet to the number of times that the node receives a packet forwarding request. Cooperation enforcement aims at increasing the rate.

- **Percentage of conditional cooperators**: the definition of this metric is as described in section 4.4.1.4.

- **Packet delivery ratio**: this metric is defined as the ratio of the total number of data packets received by destination nodes to the total number of data packets generated by all nodes in the network.

The justifications for choosing cooperation rate and percentage of conditional cooperators as performance metrics have been discussed in section 4.4.1.4. In this section, we add another performance metric i.e. packet delivery ratio. The reason for using packet delivery ratio as one of the performance metrics is that its calculation is affected by packet loss. It can occur as a result of link errors or selfish intermediate nodes intentionally drop packets that they are supposed to forward [Buchegger & Le Boudec, 2002]. High packet delivery ratio could indicate high cooperation between nodes if each packet travels through at least one intermediate node to reach destination node.

The performance of MaTaCo in TACMAN was evaluated in a series of experiments that were conducted using the JiST/SWANS simulator. This section describes the software and hardware, and the general parameters used for the simulation. The experiments are presented and their results are analyzed.

5.2.1.5 Mobility Pattern Generation

As mentioned in section 5.1.1.3, TACMAN uses RWM as the mobility model. The justification for choosing RWM has been discussed in section 4.4.1.5. In order to generate mobility patterns, we utilize the RWM patterns generator that is provided within the JiST/SWANS simulator. Given a set of parameters which defines the network size, minimum and maximum allowable speeds, pause time, area size and simulation duration, the simulator will generate mobility patterns that cause nodes to move based on the RWM model. The parameters are illustrated in table 5.1.

Parameter	Value Format	Description
Network size	Unsigned integer	Defines the total number of nodes involved in simulation
Minimum speed	Floating point	Defines the minimum speed allowed, in meters per second, for a mobile node
Maximum speed	Floating point	Defines the maximum speed allowed, in meters per second, for a mobile node
Pause time	Floating point	Defines the length of time, in seconds, for which nodes should pause before changing direction
Simulation time	Floating point	Defines the duration of simulation, in seconds, in which nodes are allowed to move
Area width	Floating point	Defines the width of simulation area, in meters
Area length	Floating point	Defines the length of simulation area, in meters

Table 5.1: A set of parameters required to generate RWM patterns. The RWM patterns generator is provided within the JiST/SWANS simulator.

5.2.1.6 Simulation Hardware and Software

MaTaCo was implemented within the JiST/SWANS simulator version 1.0.6. The simulator was chosen because it is faster and consumes less memory than other network simulators such as ns-2 and GloMoSim [Barr et al. (2005b)]. The machine specifications, operating system, SDK, JRE and compiler are as described in section 4.4.1.6.

Similar to Repast Simphony, simulation in JiST/SWANS is based on an ideal environment in which it does not include the simulation of refractions of signals on obstacles or the absorbing of signals by bodies. Thus, as discussed in section 4.4.1.6, the information fed into the approaches may differ significantly from the real world; however, it is suitable as a basis for a comparison of the approaches against each other.

5.2.1.7 Experimental Parameters

The general parameters used in experiments in this chapter i.e. number of nodes, size of area, transmission range, mobility model, simulation time, and interactions period were as described in section 4.4.1.7. The motivations for choosing the parameters have also been discussed in the section. We recall the parameters in table 5.2.

The network started with 70 percent conditional cooperators and 30 percent selfish nodes. We use 30 percent selfish nodes in order to test if the baselines could compete with MaTaCo if the selfish nodes percentage is lower than 50% at the start of simulation. IEEE 802.11

Parameter	Value
Network size	50 nodes
Minimum speed	0m/s
Maximum speed	10m/s
Pause time	30s
Simulation time	1100s
Area width	1000m
Area length	1000m
Transmission range	250m
Interaction starts at	100s
Interaction stops at	1000s
Conditional cooperators	70%
Unconditional defectors	30%
Payoff	$T = 1.9$, $R = 1$, $P = 0.0001$ and $S = 0$
MAC	IEEE 802.11 with DCF
Traffic	CBR
Packet size	512 bytes

Table 5.2: General parameters of the simulation. All experiments used the values stated in this table, unless specified otherwise.

protocol with Distributed Coordination Function (DCF) was used as the MAC protocol. The chosen transmission range and MAC represents an off-the-shelf wireless interface device [Buchegger & Le Boudec (2002)]. Traffic is at constant bit rate (CBR). By using CBR for traffic, protocol particularities of traffic protocols that are more complex, such as Transmission Control Protocol (TCP), can be avoided [Buchegger & Le Boudec, 2002]. 10 CBR flows were simulated where each flow sends four 512 bytes data packets per second. Variations in data packet size value are not expected to affect MaTaCo and the baselines, thus it remained constant for this evaluation. All results were averaged over ten runs, each with a different seed. The seed value affects the placement and movement of nodes in the simulation.

5.2.2 Experiments

A series of experiments were conducted in the JiST/SWANS simulator in order to test the hypothesis that MaTaCo promotes higher cooperation than RCA and HE in a MANET under

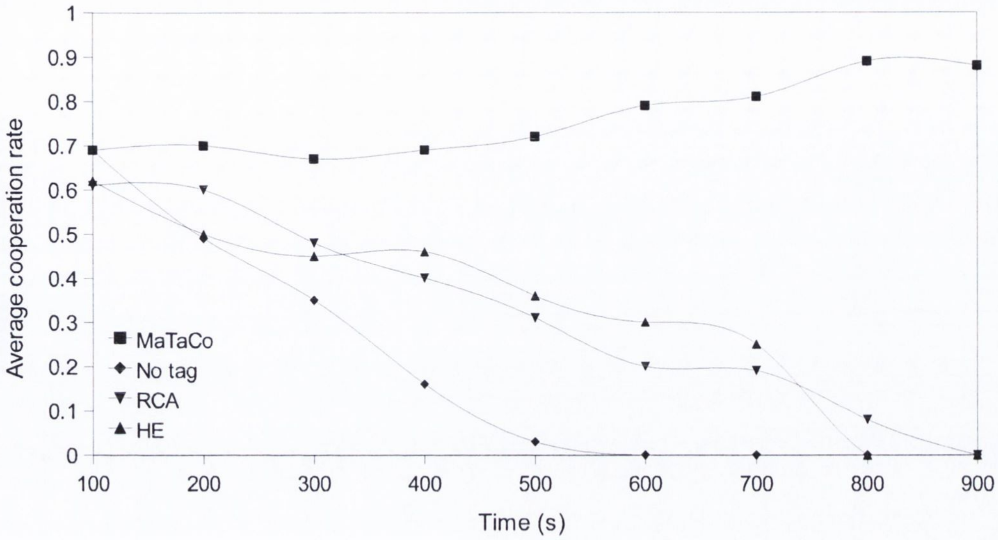

Figure 5.1: Average cooperation rate over time

varying conditions i.e. initial number of selfish nodes, speeds of nodes, network size, network density and network load. As discussed in section 4.4.2, there are two aspects in the hypothesis that need to be tested i.e. cooperation and robustness. Therefore, we test the cooperation aspect by measuring cooperation rate, percentage of conditional cooperators and packet delivery ratio of each approach, and the robustness of each approach against varying conditions by conducting different categories of experiments. In this section, we present the experiments and discuss their results.

5.2.2.1 Experiment 1: Performance over Time

This experiment evaluates the performance of MaTaCo in comparison to the baselines described before, over time. Figure 5.1 and 5.2 show the average cooperation rate and the percentage of conditional cooperators, respectively, over time for MaTaCo, No-tag, RCA and HE.

We observe that if the packet forwarding game is played without tag mechanism, as in No-tag case, the average cooperation rate and the percentage of conditional cooperators decrease to zero in 600 seconds. This supports the argument that a cooperation enforcement system

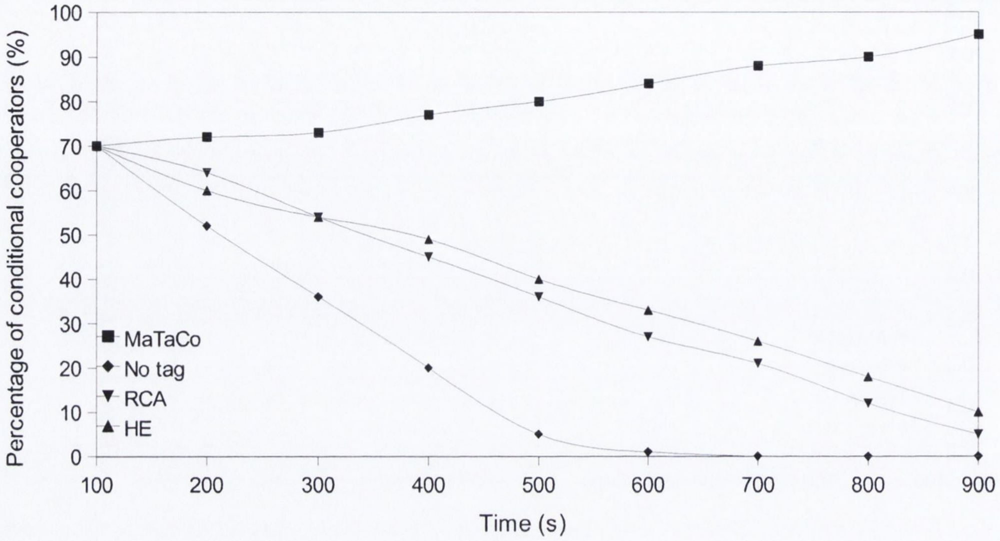

Figure 5.2: Percentage of conditional cooperators over time

such as a tag-based system is necessary in order to promote cooperation in MANETs. The results also show that RCA and HE could only lengthen the time but still could not prevent the network from reaching zero cooperation rate. In RCA and HE, the average cooperation rates drop to zero at 900 and 800 seconds, respectively. The percentages of conditional cooperators for RCA and HE drop to 4 and 6 % at the end of simulation. These findings justify the necessity of having a tag-based cooperation system that is responsive and adaptive to nodes' mobility.

Distinct from RCA and HE, MaTaCo increases the average cooperation rate and the percentage of conditional cooperators over time. Conditional cooperators increases from 70% at the start of simulation to 95% at the end of simulation, while the average cooperation rate rises from 0.62 to 0.91. This shows that MaTaCo has the capability to enforce high cooperation in MANETs. The reason it outperforms RCA and HE is as described in section 4.4.2.1.

Figure 5.3 illustrates the packet delivery ratio over time. It is observed that the packet delivery ratio depends on the average cooperation rate. High average cooperation rate results in high packet delivery ratio and vice versa. However, most of the time, the packet delivery

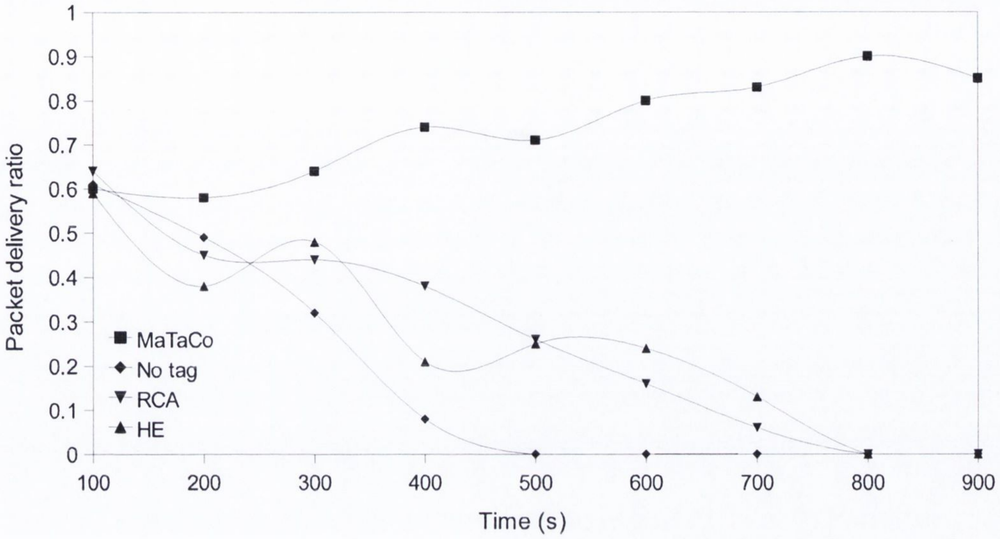

Figure 5.3: Packet delivery ratio over time

ratio could not reach as high as the average cooperation rate. This is due to unintentional packet dropping or packet loss which may occur as a result of nodes' mobility or wireless channel errors. Overall, MaTaCo increases the packet delivery ratio over time while the baselines decrease the ratio.

5.2.2.2 Experiment 2: Impact of Mobility

This experiment evaluates MaTaCo's performance in comparison to the baselines, under varying speeds of nodes. Table 5.3 lists the maximum speed settings used in four scenarios.

Scenario	Maximum speed (m/s)
1	5
2	10
3	15
4	20

Table 5.3: Maximum speed setting

The motivation for each setting has been discussed in section 4.4.2.2. The average cooperation rate, and the percentage of conditional cooperators at the end of simulation of MaTaCo

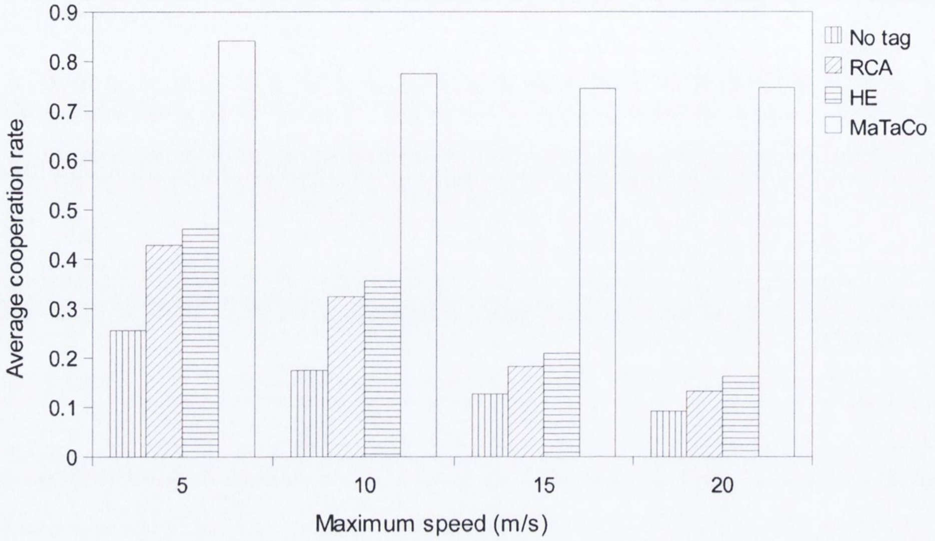

Figure 5.4: Average cooperation rate with respect to maximum speed

are compared with the implementation of No-tag, RCA and HE. Similar to the modified MaTaCo in TACME, MaTaCo is expected to produce higher average cooperation rate and percentage of conditional cooperators, as it incorporates nodes' mobility in its mechanism.

Figure 5.4 shows the average cooperation rate for a maximum speed of 5 m/s, 10 m/s, 15 m/s, and 20 m/s for MaTaCo and the baselines. It is observed that MaTaCo produces a higher average cooperation rate than the baselines in each case. With an increasing maximum speed, the average cooperation rate drops. This is because of the increase in variation of nodes' speed which decreases the probability of a node finding other nodes that have similar tags.

Figure 5.5 illustrates the percentage of conditional cooperators at the end of simulation. As mention earlier, the network has 50% conditional cooperators at the start of simulation.At the end of simulation, MaTaCo increases the percentage of conditional cooperators in the network by 27 to 30% depending on the maximum speed setting. The baselines, on the other hand, decrease the percentage of conditional cooperators in the network in each of the maximum speed setting. This is expected as the baselines were not designed for MANETs.

The results also show that even in low mobility environment i.e. 5 m/s maximum speed, the baselines are not able to increase the percentage of conditional cooperators in the network.

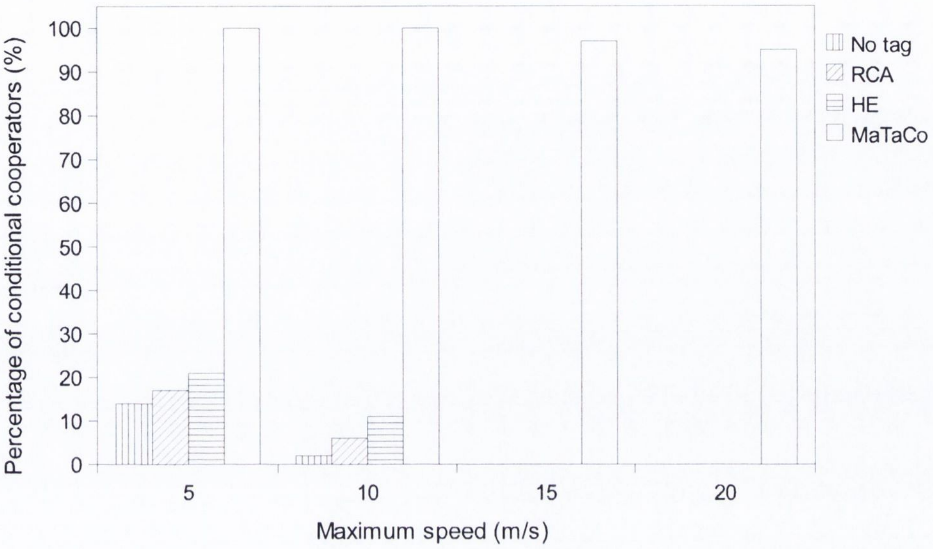

Figure 5.5: Percentage of conditional cooperators at the end of simulation with respect to maximum speed

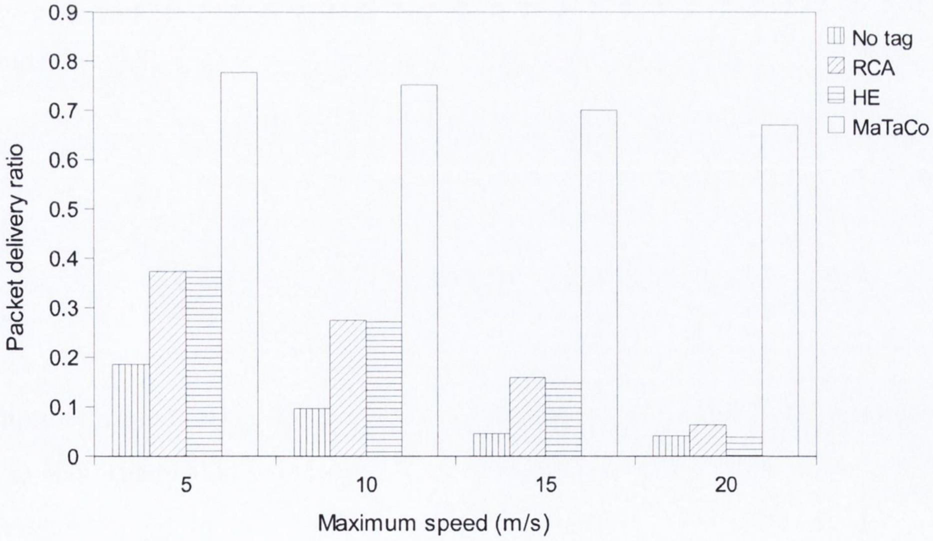

Figure 5.6: Packet delivery ratio with respect to maximum speed

MaTaCo, on the other hand, increases the percentage even in high mobility environment i.e. 20 m/s maximum speed where in that case, the percentage rises from 70% to 97%. Therefore, MaTaCo is expected to outperform No-tag, RCA and HE in all scenarios outlined in the next sections as the scenarios are fixed at 10 m/s maximum speed.

Figure 5.6 shows the packet delivery ratio with respect to maximum speed. Overall, MaTaCo increases the packet delivery ratio while the baselines decrease the ratio, in each case. The explanation on the packet delivery ratio is as described in section 5.2.2.1. Furthermore, high node mobility leads to more link breakages, which in turn results in more packets being dropped unintentionally.

5.2.2.3 Experiment 3: Impact of Selfish Nodes

This experiment evaluates the impact of varying number of selfish nodes at the start of simulation on the performance of MaTaCo in comparison to the baselines, with respect to the average cooperation rate, the percentage of conditional cooperators and packet delivery ratio. Table 5.4 lists the settings used for selfish nodes percentage at the start of simulation. Scenario 1, 2 and 3 provide a bias towards cooperative environment as each of the scenario starts with a percentage of selfish nodes that is smaller than percentage of cooperative nodes while scenario 4 ensures that there is no bias towards either cooperative or selfish environment.

Scenario	Selfish nodes (% of network size)
1	20
2	30
3	40
4	50

Table 5.4: Percentage of selfish nodes setting

Figure 5.7 and 5.8 show the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for a percentage of selfish nodes of 20%, 30%, 40% and 50%. Both figures show that the baselines do not promote higher cooperation even when the selfish nodes percentage is at the lowest setting. MaTaCo, on the other hand, increases the average cooperation rate and the percentage of conditional cooperators. However, as the percentage of selfish nodes increases, both the average cooperation rate and the

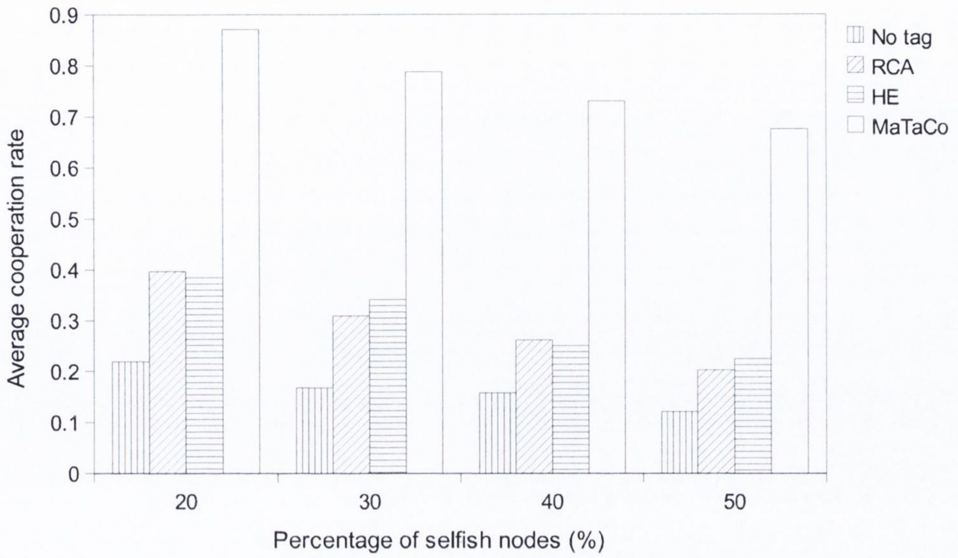

Figure 5.7: Average cooperation rate with respect to percentage of selfish nodes at the start of simulation

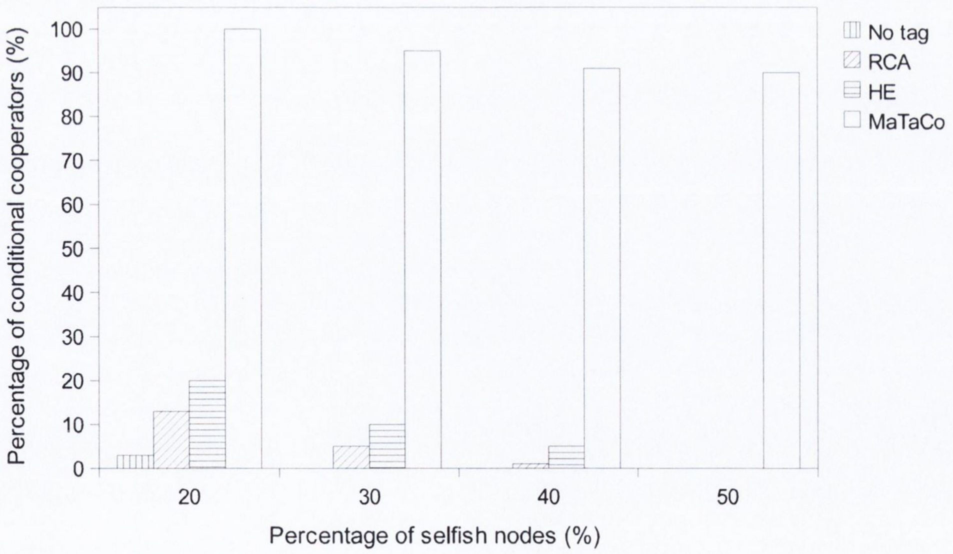

Figure 5.8: Percentage of conditional cooperators at the end of simulation with respect to percentage of selfish nodes at the start of simulation

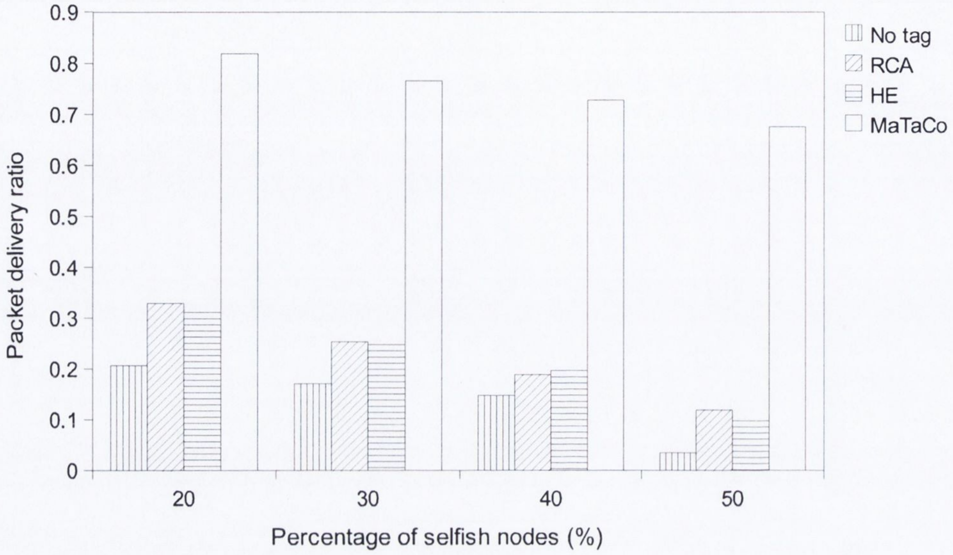

Figure 5.9: Packet delivery ratio with respect to percentage of selfish nodes at the start of simulation

percentage of conditional cooperators decrease. The average cooperation rate has a higher decrease rate than the percentage of conditional cooperators due to low cooperation rate at the early of simulation. The results also show that MaTaCo is able to increase the percentage of conditional cooperators at the end of simulation even when the network starts with 50% selfish nodes, where the percentage rises from 50% to 90%.

Figure 5.9 illustrates the packet delivery ratio with respect to selfish nodes percentage. Overall, MaTaCo outperforms the baselines with regards to the packet delivery ratio as well as the other two performance metrics. The explanation on the packet delivery ratio is as described in section 5.2.2.1.

5.2.2.4 Experiment 4: Impact of Network Size

This experiment evaluates the average cooperation rate, the percentage of conditional cooperators and packet delivery ratio, when network size varies. Table 5.5 lists the parameter settings used. Figure 5.10 and 5.11 illustrate the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for a network size of 100, 200, 300, and 400 nodes. This experiment could only support up to a maximum of 400 nodes

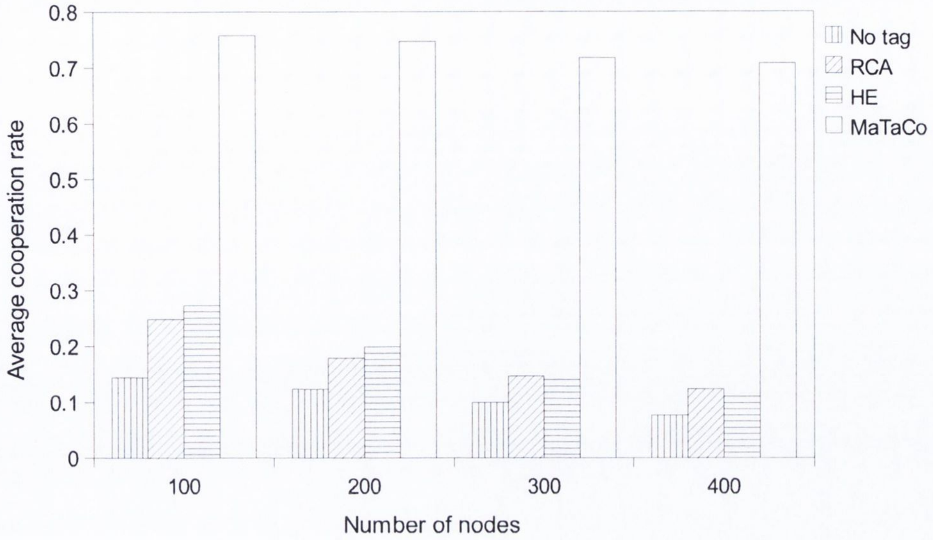

Figure 5.10: Average cooperation rate with respect to number of nodes

due to the same reason discussed in section 4.4.2.4. The network density is fixed at 20000 m^2/node (which is as same as the network density for 50 nodes in an 1000m x 1000m area) and the number of CBR flows is fixed at 20% of the network size. For instance, a network of 100 nodes requires an area of approximately 1414 x 1414 m^2 and 20 CBR flows.

Scenario	Network size	Area size (m x m)	CBR flows
1	100	1414m x 1414m	20
2	200	2000m x 2000m	40
3	300	2449m x 2449m	60
4	400	2828m x 2828m	80

Table 5.5: Parameter setting

With regards to MaTaCo, the percentage of conditional cooperators increases in each case which results in the increase of the average cooperation rate of the network. With an increasing network size, both the average cooperation rate and the conditional cooperators percentage for MaTaCo are not decreasing significantly. The reason is that the maximum speed is fixed at 10 m/s in each case, thus the probability of a node finding other nodes with similar tags does not change significantly between the cases.

Figure 5.12 shows the packet delivery ratio with respect to number of nodes. In each

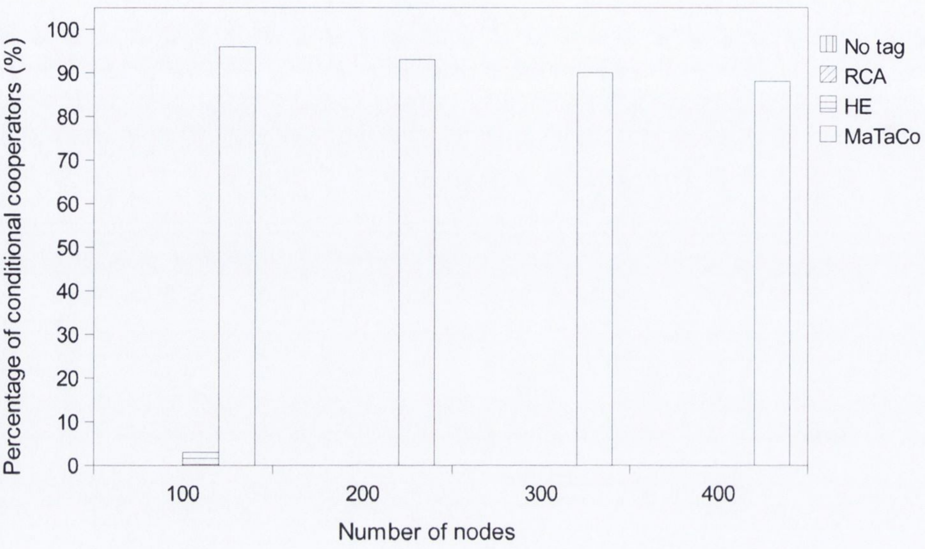

Figure 5.11: Percentage of conditional cooperators at the end of simulation with respect to number of nodes

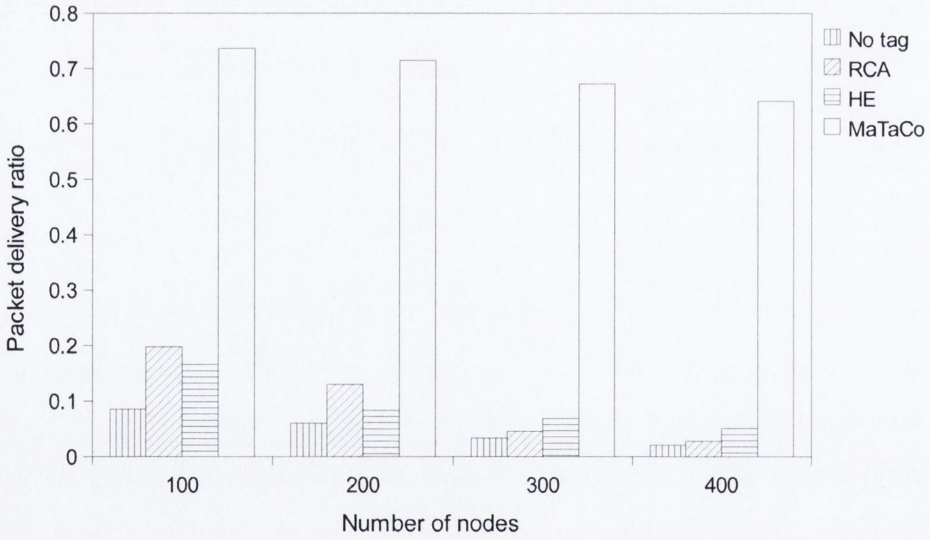

Figure 5.12: Packet delivery ratio with respect to number of nodes

case, MaTaCo increases the packet delivery ratio while the baselines decrease the ratio. The explanation on the packet delivery ratio is as described in section 5.2.2.1.

5.2.2.5 Experiment 5: Impact of Network Density

This experiment evaluates the impact of network density on the average cooperation rate, the percentage of conditional cooperators and packet delivery ratio. Table 5.6 lists the network density settings used. The simulation area size is changed accordingly to keep the network size fixed at 50 nodes. For instance, a network of 50 nodess with a density of 30000m^2/agent requires an area of 1500000m^2 which equals to approximately 1225m by 1225m square area. The justifications for the choice of network density values have been discussed in section 4.4.2.5.

Scenario	Network density (m^2/agent)	Area size (m x m)
1	10000	707m x 707m
2	20000	1000m x 1000m
3	30000	1225m x 1225m
4	40000	1414m x 1414m

Table 5.6: Population density setting

Figure 5.13 and 5.14 show the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for a network density of 10000, 20000, 30000, and 40000 m^2/agent. Figure 5.15 illustrates the packet delivery ratio with respect to number of nodes in which MaTaCo outperforms the baselines in each case. As network density decreases, we observe that the rate, the percentage and the ratio decrease. The reason is that each node's transmission range is limited to 250 m. Thus, as the network density decreases which in turn increases the network area size, the probability of a node finding neighbors decreases as the probability of nodes moving out of each other's transmission range. With a decreasing probability of a node finding neighbors, the probabilities of a node finding other nodes with similar tags and a node has a neighbor to compare its payoff with also decrease.

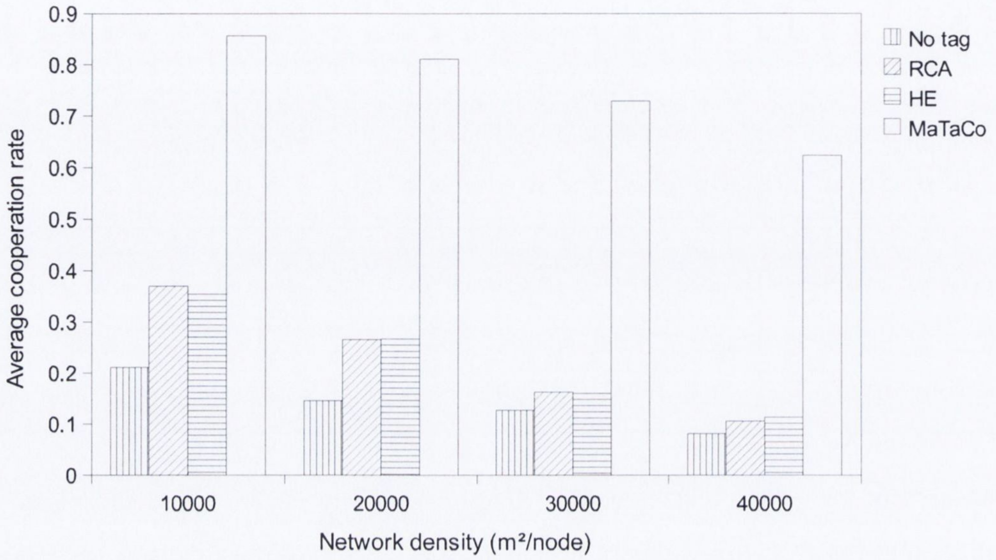

Figure 5.13: Average cooperation rate with respect to network density

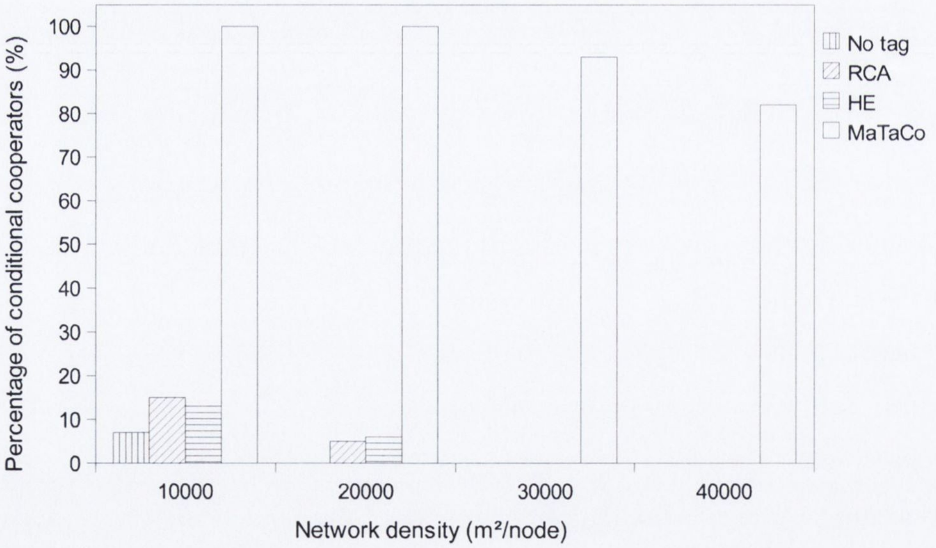

Figure 5.14: Percentage of conditional cooperators at the end of simulation with respect to network density

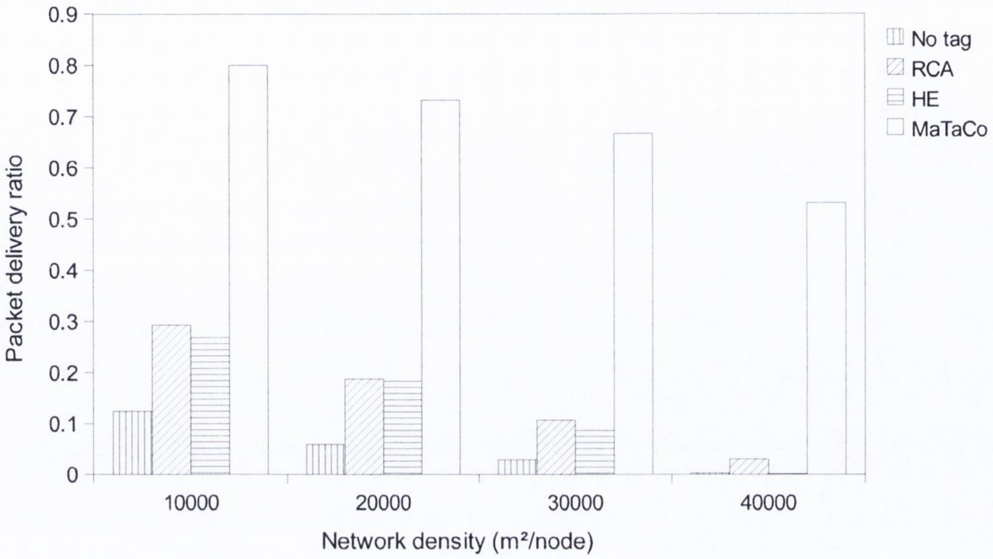

Figure 5.15: Packet delivery ratio with respect to network density

5.2.2.6 Experiment 6: Impact of Network Load

This experiment evaluates MaTaCo's performance under varying network load. Table 5.7 lists the network load settings used. Figure 5.16 and 5.17 show the average cooperation rate and the percentage of conditional cooperators at the end of simulation, respectively, for 5, 10, 15 and 20 CBR flows. The values were chosen such that they do not reach 50% of the network size (which is 50 nodes). If the number of CBR flows is 50% of the network size at a time, then each CBR flow would not have any intermediate node as each node would have to act as either sender or receiver.

Scenario	Number of CBR flows
1	5
2	10
3	15
4	20

Table 5.7: Network load setting

We observe that the increase of number of CBR flows does not affect MaTaCo's performance significantly. The average cooperation rate and the percentage of conditional coopera-

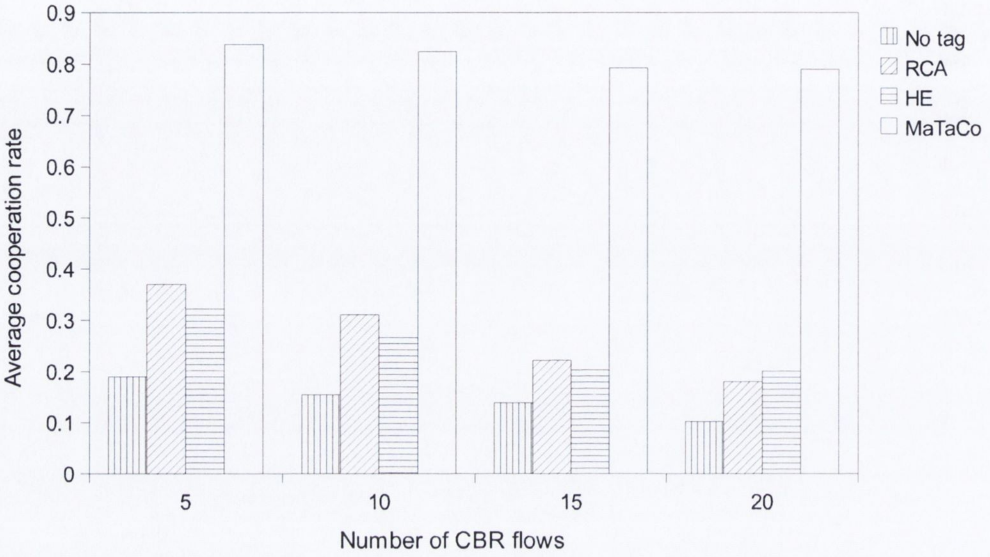

Figure 5.16: Average cooperation rate with respect to number of CBR flows

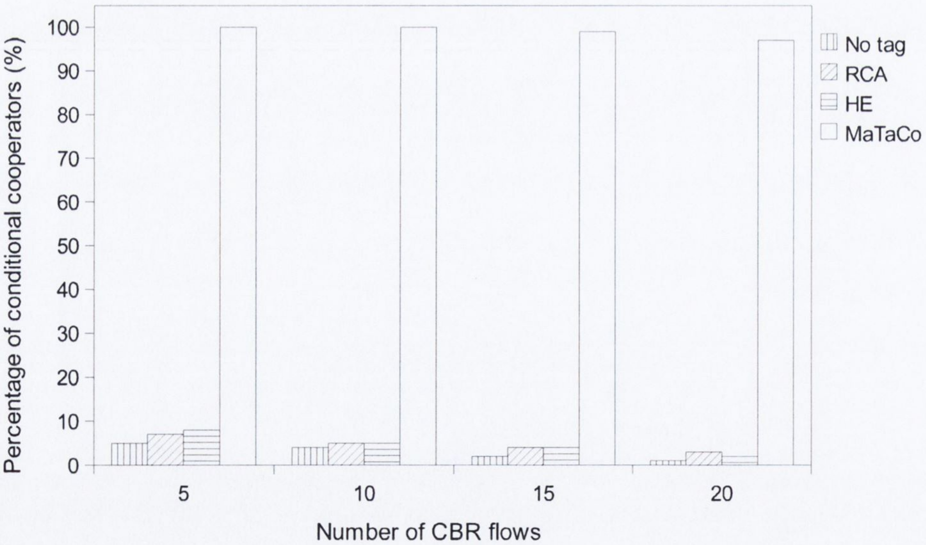

Figure 5.17: Percentage of conditional cooperators at the end of simulation with respect to number of CBR flows

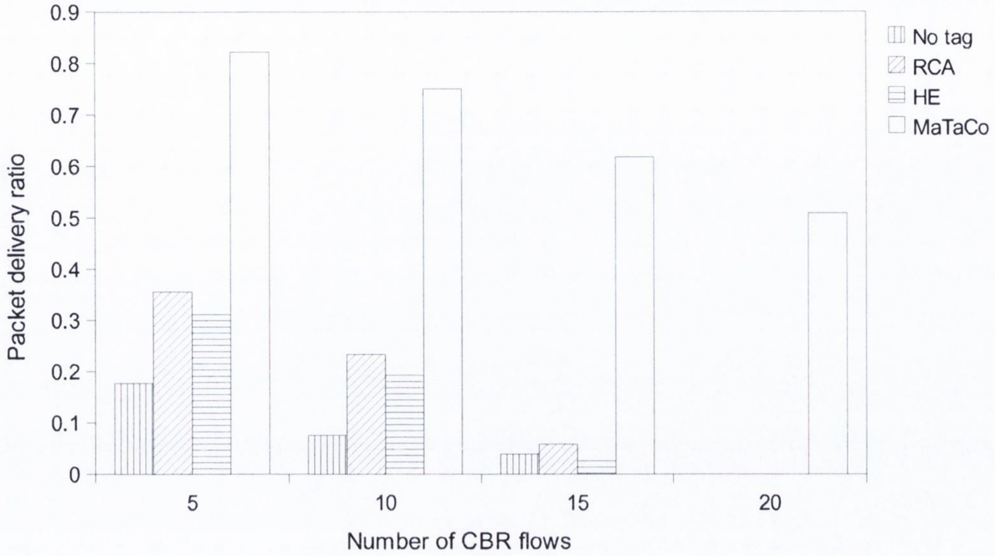

Figure 5.18: Packet delivery ratio with respect to number of CBR flows

tors decrease only slightly with an increasing number of flows. Overall, MaTaCo outperforms No-tag, RCA and HE in each case, even in the case of 20 CBR flows where it increases the percentage of conditional cooperators from 70% to 97%.

Figure 5.18 illustrates the packet delivery ratio with respect to number of CBR flows. It is observed that the decrease rate of the packet delivery ratio is higher than the average cooperation rate. The reason is that the higher the number of CBR flows, the higher the output queue overflow and channel interference, which results in more packets being dropped unintentionally.

5.3 Analysis of Overall Simulation Results

The results in TACME and TACMAN show that MaTaCo outperforms the baselines under varying conditions. In our view, the key aspect that contributes to the great performance of MaTaCo in mobile environment and a MANET, compared to the baselines, is the suitable choice of tags. Based on the principle of tag-based cooperation, the formation of local interaction groups in a population or a network is crucial in ensuring high level of cooperation between nodes in the network. This is because only with the existence of the groups that nodes have the incentives to maximize their own payoffs by cooperating. Therefore, when there are local interaction groups in a network, each node acts cooperatively in order to maximize its payoff. Selfish nodes in the network then copy the behavior of cooperative nodes as they realize that cooperative nodes are gaining higher payoff than themselves. As a result, cooperative nodes will take over the network. In order to ensure that local interaction groups can be successfully formed in a network, tags must be chosen carefully depending on the scenario that are being investigated. For instance, RCA and HE investigated scenarios of wired network in which nodes are not mobile and each of them are assumed to be able to interact with any node in the network. Therefore, the use of real numbers in RCA or lists of neighbors in HE as tags, to ensure the formation of local interaction groups in the network, is suitable as a group can be composed of nodes from anywhere in the network. However, in this thesis, we investigate scenarios of mobile environment and MANET in which nodes are mobile. They interact between them over wireless medium and their neighborhoods are limited by their transmission range. Therefore, the formation of local interaction groups depends on the movement and transmission range of nodes. Real numbers and lists of neighbors are not suitable as tags in mobile environment or MANETs as they do not capture the two factors. This causes RCA and HE to be incapable of structuring the population of mobile nodes into local interaction groups. Consequently, as the simulation results show, RCA and HE are unable to enforce high cooperation between nodes in mobile environment and a MANET. We determine that relative mobility between nodes is suitable as tags in mobile environment or MANETs as it is also affected by the movement and transmission range of nodes. This gives MaTaCo the ability to structure the population of mobile nodes into local interaction groups and consequently enforce high cooperation between nodes in TACME and TACMAN.

5.4 Summary

This chapter described the development of TACMAN, a MANET model for tag-based cooperation. In this model, the original MaTaCo approach was implemented. Hence, received power levels, $RxPr$ were used in measuring tags similarity. Mobile nodes in TACMAN played packet forwarding games between them.

This chapter also presented the evaluation of MaTaCo in TACMAN, in comparison to the No-tag, RCA and HE approaches. A set of experiments that evaluate the performance of MaTaCo in terms of enforcing higher cooperation than the baselines under varying conditions, was presented. Similar to the modified MaTaCo in TACME, MaTaCo outperformed the baselines under all tested conditions in TACMAN. MaTaCo increased the average cooperation rate, the percentage of conditional cooperators and the packet delivery ratio under varying percentage of selfish node at the start of simulation, speed of nodes, network size network density and network load. The baselines, on the other hand, decreased the rate, the percentage and the ratio under the varying conditions.

From the analysis and discussion, we conclude that MaTaCo achieves the objective of promoting higher cooperation than existing tag-based models such as RCA and HE and satisfies the requirements of being aware of nodes' transmission range limit and mobility. It also satisfies the requirement of being responsive and adaptive to varying mobile environment.

Chapter 6

Conclusions and Future Work

This thesis describes the design and implementation of MaTaCo, a novel tag-based cooperation enforcement approach for MANETs. MaTaCo realizes a mobility-aware tag-based cooperation enforcement system by providing mechanisms that respond and adapt to changing mobile environment, and utilize nodes mobility in enforcing cooperation. This chapter summarises the achievements of this thesis and its contributions, and concludes with a discussion of potential areas of future work.

6.1 Achievements

In self-organized MANETs, each node is self-interested and tempted to drop others' packets to preserve of their own limited resources such as 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 in order to mitigate the selfishness problem. An analysis of state of the art cooperation enforcement systems highlighted two main limitations that motivated the work presented in this thesis. Firstly, most of cooperation enforcement systems for MANETs require each node to maintain memory of past interactions. This requirement can be a significant problem in open and large mobile ad hoc networks. To address this problem, the requirement of memory of past interactions must be removed; in other words cooperation without reciprocity needs to be achieved. Cooperation without reciprocity has been investigated by researchers from a number of fields and the common idea they share is the use of tag-based mechanisms to enforce cooperation. Secondly, existing tag-based cooperation enforcement systems do not target mobile environment such as MANETs. Therefore, a new tag-based cooperation enforcement system is needed.

A tag-based cooperation enforcement system targeting MANETs should be able to respond and adapt to changing mobile environment. A primary challenge of this work is on how to develop a tag-based cooperation enforcement system that is mobility-aware. Chapter 3 described the design of MaTaCo, a mobility-aware tag-based cooperation approach for MANETs. MaTaCo is designed to take into account nodes' mobility and limited transmission range. The focus of the work was on the incorporation of nodes' mobility into the approach. The main contribution of the work is the use of a mobility metric that links a node's tag to its mobility and gives MaTaCo an ability to respond and adapt to changing mobile environment.

The development of an abstract, mobile environment model for tag-based cooperation was described in Chapter 4. In the model, mobile nodes and a packet forwarding session in MANETs are generalized as mobile agents that have limited view radius and a PD game, respectively. Therefore, mobile agents in the model interact between them in PD games. As there was no wireless communication involved in the model, MaTaCo was modified to use distances between agents, instead of received power levels, in the mobility metric. The evaluation of the modified MaTaCo was also presented in the chapter. Five experiments were conducted against the implementation of the modified MaTaCo, as well as implementations of existing tag-based approaches i.e., RCA and HE. The experiments were also conducted without any tag-based mechanism. The experiments differ in the values of parameters used, such as agents' maximum speeds, selfish agents percentages at the start of simulation, population sizes and population densities. Values for these parameters are taken from existing work that evaluates cooperation enforcement system in MANETs. The results highlight two findings; first, the modified MaTaCo outperforms the implementations of RCA and HE in all experiments and second, RCA and HE, on the other hand, cannot enforce cooperation in mobile environment.

The development of a MANET model for tag-based cooperation was presented in Chapter 5. Distinct from the previous model, this model simulates a MANET environment. Experiments similar to the previous model were conducted against the implementation of original MaTaCo approach. As expected, the results are similar to those obtained from the previous model, in which MaTaCo outperforms the other approaches under all conditions.

In our view, the great performance of MaTaCo, compared to the baselines, is due to the use of relative mobility between nodes as tags. In MANETs where nodes are mobile, the relative mobility between nodes contributes in structuring the population of mobile nodes as it captures the formation of local interaction groups in the presence of nodes' mobility. The population is divided into groups based on their relative mobility where mobile nodes that are moving closer to each other formed a local interaction group. Based on the principle of tag-based cooperation, as explained in section 2.5, if a node wants to maximize its own payoffs, it has to cooperate in its local interaction group. Thus, each mobile node choose to cooperate over defect. Selfish nodes in the network will copy cooperative nodes behavior as they discover that cooperative nodes gain higher average payoffs than themselves. Subsequently, cooperative nodes will take over the network. This mechanism makes MaTaCo's performance greater than the baselines. Although RCA and HE are also based on the principle of tag-based cooperation, what makes MaTaCo distinct from them is the use of relative mobility between nodes as tags. The results show that by using the relative mobility between mobile nodes, they can be structured into groups. Structuring population into groups is one of the important aspects that makes a tag-based approach successful. If there is no local interaction group in the population, then there is no reason for a node to cooperate as it does not guarantee to maximize its own payoff. While the use of real numbers in RCA and lists of neighbors in HE can divide a population of stationary nodes into groups, they are incapable of structuring population of mobile nodes as the simulation results show.

In summary, the research presented in this thesis focused on providing a tag-based cooperation enforcement approach that is capable of enforcing high cooperation in changing mobile environment. The main contributions of this thesis are summarized as:

- An overview of existing cooperation enforcement models targeting MANETs. The models are evaluated with a particular focus on their characteristics. Limitations of the models are identified, which motivated the research to investigate further on tag-based cooperation.

- An overview of existing tag-based cooperation enforcement models. The models are analyzed based on their characteristics. Selected concepts from these tag-based models, such as the tag, strategy as well as reproduction mechanisms, were influential for our approach's design.

- A mobility-aware tag-based cooperation enforcement approach for MANETs named MaTaCo. MaTaCo incorporates nodes' mobility into its tag mechanism which makes it responsive to the non-stationary nature of MANETs while its two traits of strategy makes it adaptive to the environment. Compared to existing cooperation enforcement approaches for MANETs, MaTaCo does not require keeping memory of past interactions such as observation logs and reputation records. Hence, there is no need for each node to have a monitoring mechanism and a unique identity linked to the behavior of each node. Compared to existing tag-based models for wired networks, MaTaCo takes into account the mobility of nodes and their limited transmission range. Therefore, it is suitable for applications whereby the agents in the environment are moving and have incomplete information about the environment.

- The implementation and evaluation of MaTaCo in a mobile environment as well as a MANET model. The evaluation shows that MaTaCo is beneficial for both mobile and MANET environment. MaTaCo is compared to implementations of existing tag-based models i.e. RCA and HE. The evaluation confirms that higher average cooperation rate, percentage of conditional cooperators at the end of simulation, as well as packet delivery ratio are achieved by MaTaCo than by RCA and HE.

- A new class of cooperation enforcement approaches for MANETs. Existing models can be classified as credit-, reputation- and game-based approaches, while MaTaCo can be classified as a tag-based approach.

6.2 Future Work

Future work should investigate a number of issues, with the aim to further improve the performance of MaTaCo. This section outlines the key areas identified for future work.

The proposed approach assumes that selfish nodes refuse to forward data packets but participate in route discovery and maintenance. Future work should also consider selfish nodes that refuse to participate in both routing and forwarding, and selfish nodes that behave according to their energy level as described in section 1.2. Thus, the effects of different selfish behaviors can be studied.

The experiments presented in this thesis are limited to 1000 seconds of simulation time. Future work should remove the simulation time limit and investigate whether steady-state cooperation can be achieved by employing MaTaCo. Moreover, techniques to decrease the time needed to enforce full cooperation should also be investigated.

The proposed approach also assumes that all nodes do not deviate from MaTaCo's algorithm. Future work should consider the presence of cheaters. A cheater could advertise fake payoff and strategy when comparing payoff. Therefore, the performance of MaTaCo in the presence of cheaters should be assessed in future work.

The impact of other factors such as number of neighbors, time interval for comparing payoff as well as frequency of hello messages on the performance of MaTaCo should be evaluated, with the aim to provide a thorough evaluation of the approach.

As the evaluation of MaTaCo in this thesis is simulation-based, future work should further investigate the implementation of MaTaCo in real world experiments. The reason is that simulation environment may not capture all factors that affect the performance of MaTaCo in real world [Kiess & Mauve (2007)]. Next section discusses a program of research that can be conducted in order to assess MaTaCo and the significance of its performance in real world scenarios.

6.2.1 Real World Experiments

A real world experiment involves deploying and testing a proposed approach in a real-time network under realistic conditions, e.g. using real wireless communication links and nodes mobility, and complying with devices specifications [Kropff et al. (2006)]. In order to conduct real world experiments for MaTaCo, a MANET testbed has to be implemented. Therefore, the first step is to identify a suitable tool to implement a MANET testbed for the evaluation of MaTaCo.

There are many tools that have been developed in order to implement a testbed e.g. Airplug-emu, Castadiva, ManetLab, MiNT, mLab, MobiEmu, ORBIT, RoofNet, TrueMobile and WHYNET [Vessaz et al. (2013)]. They should be assessed, in order to determine the best testbed for evaluating MaTaCo, in terms of whether they support multi-hop communication and their availability [Vessaz et al. (2013)]. The availability of each tool can be determined by assessing its online download availability, if its source code and complete documentation are provided and if it requires specialized hardware for testbed implementation. For MaTaCo evaluation, we require a tool that support multi-hop communication, can be downloaded online, provides its source code and complete documentation, and can be run on standard mobile devices, laptops or desktops. Moreover, the tool should also support realistic nodes mobility. When the tool has been identified, the next step is to implement MANET routing protocol and MaTaCo on the testbed. Besides AODV, the research should also consider other routing protocol such as Optimized Link State Routing (OLSR) protocol [Clausen & Jacquet (2003)]. These two routing protocols are different in that AODV is a reactive protocol while OLSR is a proactive protocol. It is interesting to see how MaTaCo performs in different types of routing protocols.

The implementation of testbed alone is not enough to provide real world scenarios. A real MANET application should be implemented on the testbed such as P2P content sharing application in order to assess MaTaCo in real world scenarios. A good example of P2P content sharing for MANETs is BitHoc protocol [Krifa (2012)]. It works similar as BitTorrent protocol but takes into account the nature of MANETs. It utilizes OLSR protocol for connectivity between nodes and supports multi-hop communication. Previously, it has been evaluated in a network composed of seven personal digital assistants and seven smart phones. In the evaluation, the author suggested two metrics to evaluate BitHoc, i.e. average download time and average sharing ratio. The sharing ratio measures the total amount of uploads over the total amount of downloads of a node, where a value of one indicates that the node uploads and downloads equally.

As BitHoc requires cooperation between nodes in order to successfully share contents between nodes, it would be interesting to reimplement BitHoc in scenarios in which selfish nodes exist. The underlying routing protocol, that BitHoc depends on to ensure connectivity between nodes, can be combined with MaTaCo in order to assess MaTaCo's performance. We would also need to implement BitHoc on AODV (that is combined with MaTaCo) since BitHoc only use OLSR as routing protocol. In order to evaluate MaTaCo, a baseline have to be established by running BitHoc on AODV or OLSR without MaTaCo. Then the outcome of running BitHoc on AODV or OLSR, combined with MaTaCo would be compared to the baseline. If the outcome produces an increase in the average sharing ratio compared to the baseline especially if the ratio value is equal or more than one, then this would indicate that MaTaCo is able to enforce cooperation between nodes in a real world scenario. In addition to the two metrics, the metrics used in this thesis, i.e. average cooperation rate, percentage of conditional cooperators and packet delivery ratio, would also be measured.

6.3 Summary

This chapter summarized the achievements of the work presented in this thesis. It outlined how this work contributed to the state of the art in cooperation enforcement approaches targeting MANETs by providing MaTaCo, a mobility-aware tag-based cooperation enforcement approach. The responsiveness of MaTaCo to changing mobile environment is realized by the incorporation of nodes' mobility in its tag mechanism while the adaptiveness of MaTaCo to the environment is realized by the provision of two traits of strategy for each node. Experiments conducted in a mobile environment model as well as a MANET model indicate that MaTaCo leads to higher cooperation between agents or nodes. This chapter concluded with suggestions for future work arising from the research undertaken in relation to this thesis.

Bibliography

Alexander, R. D. (1987). *The biology of moral systems*. Piscataway, NJ, USA: Aldine Transaction. 2.4.5

Altman, E., Kherani, A. A., Michiardi, P., & Molva, R. (2005). Non-cooperative forwarding in ad-hoc networks. In *Proceedings. of the 4th International Networking Conference*, (pp. 486–498). Waterloo, ON, Canada. 2.3

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. 1.2, 2.2.1.1, 2.2.1.1, 2.3.1.4

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). 2.5

Aschenbruck, N., Ernst, R., Gerhards-Padilla, E., & Schwamborn, M. (2010). Bonnmotion - a mobility scenario generation and analysis tool. In *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques (SIMUTools 2010)*, (pp. 1–10). Malaga, Spain. 4.2

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). 2.5

Barr, R. (2005). Jist / swans - java in simulation time / scalable wireless ad hoc network

simulator.
URL http://jist.ece.cornell.edu/sw.html 4.4.1.5

Barr, R., Haas, Z., & Renesse, R. (2005a). Jist: An efficient approach to simulation using virtual machines. *Software Practice and Experience*, *35*(6), (pp. 539–576). 5.2

Barr, R., Haas, Z., & Renesse, R. (2005b). Scalable wireless ad hoc network simulation. In J. Wu (Ed.) *Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks*. CRC Press. 5.2, 5.2.1.6

Basu, P., Khan, N., & Little, T. D. C. (2001). A mobility based metric for clustering in mobile ad hoc networks. In *Proceedings of the 21st International Conference on Distributed Computing Systems (ICDCS 2001)*, (pp. 413–418). Phoenix, AZ, USA. 3.2, 3.3.1.1, 3.3.1.1

Blazevic, L., Buttyan, L., Capkun, S., Giordano, S., Hubaux, J.-P., & Le Boudec, J.-Y. (2001). Self organization in mobile ad hoc networks: the approach of Terminodes. *IEEE Communications Magazine*, *39*(6), (pp. 166–174). 1.1

Bonabeau, E. (2002). Agent-based modeling: methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences of the United States of America*, *99*(3), (pp. 7280–7287). 4.1

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. 1.2, 2.2.2.1, 2.2.2.1, 2.2.2.1, 2.3.2.2, 2.4.5, 4.4.1.7, 5.2.1.4, 5.2.1.7

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. 1.2, 2.2.1.1, 2.2.1.1

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. 1.2, 2.2.1.1, 2.3.1.1

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). 1.1, 1.2, 2.2.1.1, 2.2.1.1, 2.3.1.1

Camp, T., Boleng, J., & Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communication and Mobile Computing: Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, *2*(5), (pp. 483–502). 4.3.1.3

Chakeres, I. D., & Royer, E. M. (2002). The utility of hello messages for determining link connectivity. In *5th International Symposium on Wireless Personal Multimedia Communications (WPMC 2002)*, (pp. 504–508). Honolulu, Hawaii, USA. 5.2.1.1

Chen, T., Wu, F., & Zhong, S. (2011). Fits: A finite-time reputation system for cooperation in wireless ad hoc networks. *IEEE Transactions on Computers*, *60*(7), (pp. 1045–1056). 1.1.1.2, 2.3

Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol (olsr). Internet Request for Comments 3626. 6.2.1

Crowcroft, J., Gibbens, R., Kelly, F., & Ostring, S. (2004). Modelling incentives for collaboration in mobile ad hoc networks. *Performance Evaluation*, *57*(4), (pp. 427–439). 2.3

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. 1.2, 2.4.2

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). 1.2, 2.2.3.1, 2.2.3.1, 2.2.3.1, 2.3.3.2

Frankel, M. S. (1982). Advanced technology testbeds for distributed, survivable command, control and communications. In *Proceedings of Military Communications Conference*

- *Progress in Spread Spectrum Communications (MILCOM 1982)*, (pp. 10.2–1–10.2–13). Boston, MA, USA. 1.1

Friis, H. T. (1946). A note on a simple transmission formula. *Proceedings of the Institute of Radio Engineers*, *34*(5), (pp. 254–256). 4.3.1.1

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. 2.5, 2.5.2.3, 2.5.3, 3.4, 4.4.1.2, 4.4.1.4

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). 2.5, 2.5.1.1, 2.5.2.2, 2.5.3, 3.4, 4.4.1.2, 4.4.1.4, 4.4.1.7

Hammond, R. A., & Axelrod, R. (2006a). Evolution of contingent altruism when cooperation is expensive. *Theoretical Population Biology*, *69*(3), (pp. 333–338). 2.5, 2.5.3, 3.3.1.1

Hammond, R. A., & Axelrod, R. (2006b). The evolution of ethnocentrism. *Journal of Conflict Resolution*, *50*(6), (pp. 926–936). 2.5

He, Q., Wu, D., & Khosla, P. (2004). Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks. In *Wireless Communications and Networking Conference (WCNC 2004)*, (pp. 825–830). Atlanta, GA, USA. 2.3

Henrich, J. (2004). Cultural group selection, coevolutionary processes and large-scale cooperation. *Journal of Economic Behavior and Organization*, *53*(1), (pp. 3–35). 2.5.3

Heppenstall, A. J., Evans, A. J., & Birkin, M. H. (2005). A hybrid multi-agent/spatial interaction model system for petrol price setting. *Transactions in GIS*, *9*(1), (pp. 35–51). 4.1

Holland, J. H. (1995). *Hidden order: how adaptation builds complexity*. New York, NY, USA: Addison-Wesley. 2.5.1.1

Hu, J., & Burmester, M. (2006). Lars: a locally aware reputation system for mobile ad hoc networks. In *Proceedings of the ACM 44th Annual Southeast Regional Conference*, (pp. 119–123). Melbourne, FL, USA. 2.3

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. 2.4.1

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). 2.5

Inchiosa, M. E., & Parker, M. T. (2002). Overcoming design and development challenges in agent-based modeling using ascape. *Proceedings of the National Academy of Sciences of the United States of America*, *99*(3), (pp. 7304–7308). 4.2

Jacob, C., Litorco, J., & Lee, L. (2004). Immunity through swarms: agent-based simulations of the human immune system. *Lecture Notes in Computer Science*, *3239*, (pp. 400–412). 4.1

Jansen, V. A. A., & Baalen, M. V. (2006). Altruism through beard chromodynamics. *Nature*, *440*, (pp. 663–666). 2.5

Janzadeh, H., Fayazbakhsh, K., Dehghan, M., & Fallah, M. S. (2009). A secure credit-based cooperation stimulating mechanism for {MANETs} using hash chains. *Future Generation Computer Systems*, *25*(8), (pp. 926–934). 1.1.1.2, 2.3

Jaramillo, J. J., & Srikant, R. (2007). 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 2007)*, (pp. 87–98). Montreal, Canada. 1.1.1.2, 2.3

Ji, Z., Yu, W., & Liu, K. (2010). A belief evaluation framework in autonomous manets under noisy and imperfect observation: vulnerability analysis and cooperation enforcement. *IEEE Transactions on Mobile Computing*, *9*(9), (pp. 1242–1254). 1.2

Jubin, J., & Tornow, J. D. (1987). Darpa packet radio network protocols. *Proceedings of the IEEE*, *75*(1), (pp. 21–32). 1.1

Kiess, W., & Mauve, M. (2007). A survey on real-world implementations of mobile ad-hoc networks. *Ad Hoc Networks*, *5*(3), (pp. 324–339). 6.2

Krifa, A. (2012). *Towards better content dissemination applications for disruption tolerant network*. Ph.D. thesis, University of Nice-Sophia Antipolis. 6.2.1

Kropff, M., Krop, T., Hollick, M., Mogre, P., & Steinmetz, R. (2006). A survey on real world and emulation testbeds for mobile ad hoc networks. In *Proceedings of 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TRIDENTCOM 2006)*, (pp. 448–453). Barcelona, Spain. 6.2.1

Kusyk, J., Sahin, C. S., Uyar, M. U., Urrea, E., & Gundry, S. (2011). Self-organization of nodes in mobile ad hoc networks using evolutionary games and genetic algorithms. *Journal of Advanced Research*, *2*(3), (pp. 253–264). 1.1.1.2, 2.3

Lee, K., Hong, S., Kim, S. J., Rhee, I., & Chong, S. (2009). Slaw: A new mobility model for human walks. In *Proceedings of the 28th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2009)*, (pp. 855–863). Rio de Janeiro, Brazil. 4.4.1.5

Lehmann, L., & Perrin, N. (2002). Altruism, dispersal, and phenotype-matching kin recognition. *American Naturalist*, *159*(5), (pp. 451–468). 2.5

Li, F., Yang, Y., & Wu, J. (2010). Attack and flee: game-theory-based analysis on interactions among nodes in manets. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, *40*(3), (pp. 612–622). 1.1.1.2, 2.3

Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in manets. *IEEE Transactions on Mobile Computing*, *6*(5), (pp. 536–550). 2.3

Liu, Y., Li, K., Jin, Y., Zhang, Y., & Qu, W. (2011). A novel reputation computation model based on subjective logic for mobile ad hoc networks. *Future Generation Computer Systems*, *27*(5), (pp. 547–554). 1.1.1.2, 2.3

Lu, R., Lin, X., Zhu, H., Zhang, C., Ho, P., & Shen, X. (2008). A novel fair incentive protocol for mobile ad hoc networks. In *Wireless Communications and Networking Conference (WCNC 2008)*, (pp. 3237–3242). Las Vegas, NV, USA. 1.1.1.2, 2.3

Luke, S., Revilla, C. C., Panait, L., Sullivan, K., & Balan, G. (2005). Mason: a multi-agent simulation environment. *Simulation: Transactions of the Society for Modeling and Simulation International*, *82*(7), (pp. 517–527). 4.2

Macal, C. M., & North, M. J. (2005). Tutorial on agent-based modeling and simulation. In *Proceedings Of The IEEE 2005 Winter Simulation Conference (WSC 2005)*. Piscataway, NJ, USA. 4.1

MacKenzie, A. B., & DaSilva, L. A. (2006). *Game theory for wireless engineers (Synthesis Lectures on Communications)*. San Rafael, CA, USA: Morgan & Claypool. 1.1.1.1

Mahmoud, M., & Shen, X. (2011). Esip: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks. *IEEE Transactions on Mobile Computing*, *10*(7), (pp. 997–1010). 1.1.1.2, 2.3

Mahmoud, M., & Shen, X. (2012). Fescim: Fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks. *IEEE Transactions on Mobile Computing*, *11*(5), (pp. 753–766). 1.1.1.2, 2.3, 2.4.1

Mahmoud, M., & Shen, X. (2013). A secure payment scheme with low communication and processing overhead for multihop wireless networks. *IEEE Transactions on Parallel and Distributed Systems*, *24*(2), (pp. 209–224). 1.1.1.2, 2.3, 2.4.1

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. 1.2, 2.2.2.1, 2.2.2.1, 2.2.2.1, 2.3.2.1

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). 2.5

Mähönen, P., Petrova, M., & Riihijärvi, J. (2006). Cooperation in ad-hoc networks. In F. H. Fitzek, & M. D. Katz (Eds.) *Cooperation in Wireless Networks: Principles and Applications*, (pp. 189–222). Dordrecht, Netherlands: Springer. 1.1.1.2

Michiardi, P., & Molva, R. (2002a). 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. 1.2, 2.2.2.1, 2.2.2.1, 2.3.2.3

Michiardi, P., & Molva, R. (2002b). Simulation-based analysis of security exposures in mobile ad hoc networks. In *Proceedings of the European Wireless Conference 2002*. Florence, Italy. 1.2, 5.2.1.1

Miller, B. W., Hwang, C. H., Torkkola, K., & Massey, N. (2003). An architecture for an intelligent driver support system. In *IEEE Intelligent Vehicles Symposium (IV 2003)*, (pp. 639–644). Columbus, OH, USA. 4.1

Minar, N., Burkhart, R., Langton, C., & Askenazi, M. (1996). The swarm simulation system: a toolkit for building multi-agent simulations. Working paper 96-06-042, Santa Fe Institute. 4.2

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. 1.2, 2.2.2.1, 2.2.2.1

Nash, J. (1951). Non-cooperative games. *The Annals of Mathematics*, *54*(2), (pp. 286–295). 2.2.3.1

North, M. J., Howe, T. R., Collier, N. T., & Vos, J. R. (2007). A declarative model assembly infrastructure for verification and validation. In S. Takahashi, D. Sallach, & J. Rouchier (Eds.) *Advancing Social Simulation: The First World Congress*, (pp. 129–140). Heidelberg, Germany: Springer. 4.2, 4.4.2

Osborne, M. J., & Rubinstein, A. (1997). *A course in game theory*. Cambridge, MA, USA: MIT Press. 1.2, 2.2.3.1, 4.3.2.1

Parker, D. C., Manson, S. M., Janssen, M. A., Hoffmann, M. J., & Deadman, P. (2003). Multiagent systems for the simulation of land-use and land-cover change: a review. *Annals of the Association of American Geographers*, *93*(2), (pp. 314–337). 4.1

Parker, M. T. (2001). What is ascape and why should you care? *Journal of Artificial Societies and Social Simulation*, *4*(1).
URL `http://jasss.soc.surrey.ac.uk/4/1/5.html` 4.2

Parry, H., Evans, A., & Morgan, D. (2006). Aphid population dynamics in agricultural landscapes: an agent-based simulation model. *Ecological Modelling*, *199*(4), (pp. 451–463). 4.1

Peirce, M. (2000). *Multi-Party Electronic Payments for Mobile Communications*. Ph.D. thesis, University of Dublin, Trinity College. 2.4.1

Perkins, C. E., & Royer, E. M. (1999). Ad hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, (pp. 90–100). New Orleans, LA, USA. 5.2.1.1

Refaei, M. T., Srivastava, V., Dasilva, L., & Eltoweissy, M. (2005). A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In *The 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005)*, (pp. 3–11). San Diego, CA, USA. 2.3, 2.4.2

Richerson, P. J., Boyd, R. T., & Henrich, J. (2003). Cultural evolution of human cooperation. In P. Hammerstein (Ed.) *Genetic and cultural evolution of cooperation*, (pp. 357–388). Cambridge, MA, USA: MIT Press. 1.1.1.1

Riolo, R. L., Cohen, M. D., & Axelrod, R. (2001). Evolution of cooperation without reciprocity. *Nature*, *414*(6862), (pp. 441–443). 2.5, 2.5.1.1, 2.5.2.1, 2.5.2.3, 2.5.3, 3.3.1.1, 3.3.1.2, 3.4, 4.4.1.2, 4.4.1.4

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*, 1244–1249. Austin, TX, USA. 2.5

Song, C., & Zhang, Q. (2009). Coffee: A context-free protocol for stimulating data forwarding in wireless ad hoc networks. In *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, (pp. 1–9). Rome, Italy. 1.2, 2.2.3.2, 2.3.4.2, 2.4.4

Spector, L., & Klein, J. (2006). Genetic stability and territorial structure facilitate the evolution of tag-mediated altruism. *Artificial Life*, *12*(4), (pp. 553–560). 2.5

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. 1.2, 2.2.3.1, 2.2.3.1, 2.2.3.1, 2.3.3.1, 2.3.3.2, 2.4.3

Sundaramurthy, S., & Belding-Royer, E. (2003). The ad-mix protocol for encouraging participation in mobile ad hoc networks. In *Proceedings of the 11th IEEE International Conference on Network Protocols*, (pp. 156–167). Atlanta, GA, USA. 1.2, 2.2.3.2, 2.3.4.1, 2.4.4

Traulsen, A., & Schuster, H. G. (2003). Minimal model for tag-based cooperation. *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, *68*(4), 046129. 2.5

Trivers, R. L. (1971). The evolution of reciprocal altruism. *The Quarterly Review of Biology*, *46*(1), (pp. 35–57). 2.4.5

Turner, A., & Penn, A. (2002). Encoding natural movement as an agent-based system: an investigation into human pedestrian behaviour in the built environment. *Environment and Planning B*, *29*(4), (pp. 473–490). 4.1

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. 1.2, 2.2.3.1, 2.2.3.1, 2.3

Vessaz, F., Garbinato, B., Moro, A., & Holzer, A. (2013). Developing, deploying and evaluating protocols with manetlab. In V. Gramoli, & R. Guerraoui (Eds.) *Networked Systems*, vol. 7853 of *Lecture Notes in Computer Science*, (pp. 89–104). Springer Berlin Heidelberg. URL `http://dx.doi.org/10.1007/978-3-642-40148-0_7` 6.2.1

Wang, K., Wu, M., Ding, C., & Lu, W. (2010). Game-based modeling of node cooperation in ad hoc networks. In *Proceedings of the 19th Annual Wireless and Optical Communications Conference (WOCC 2010)*, (pp. 1–5). Shanghai, China. 1.1.1.2, 2.3

Wei, Y., & Liu, K. J. R. (2008). Secure cooperation in autonomous mobile ad-hoc networks under noise and imperfect monitoring: a game-theoretic approach. *IEEE Transactions on Information Forensics and Security*, *3*(2), (pp. 317–330). 1.1.1.2, 1.2, 2.3, 2.4.3

Wooldridge, M., & Jennings, N. R. (1995). Intelligent agents: Theory and practice. *The Knowledge Engineering Review*, *10*(2), (pp. 115–152). 4.1

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. 2.4.2

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. 1.2, 2.2.1.1, 2.2.1.1, 2.2.1.1, 2.3.1.3

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). 1.1.1.2, 1.2, 2.2.3.1, 2.2.3.1, 2.2.3.1, 2.3.3.3, 2.4.3

Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Securing mobile ad hoc networks with certificateless public keys. *IEEE Transactions on Dependable and Secure Computing*, *3*(4), (pp. 386–399). 1.2

Zhang, Y., Lou, W., Liu, W., & Fang, Y. (2007). A secure incentive protocol for mobile ad hoc networks. *Wireless Network*, *13*(5), (pp. 569–582). 1.1.1.2, 2.3, 2.4.1

Zhao, S., Aggarwal, A., Frost, R., & Bai, X. (2012). A survey of applications of identity-based cryptography in mobile ad-hoc networks. *IEEE Communications Surveys & Tutorials*, *14*(2), (pp. 380–400). 1.2

Zhao, S., Kent, R., & Aggarwal, A. (2013). A key management and secure routing integrated framework for mobile ad-hoc networks. *Ad Hoc Networks*, *11*(3), (pp. 1046–1061). 1.2

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. 1.2, 2.2.1.1, 2.2.1.1, 2.2.1.1, 2.3.1.2, 2.4.1