Presented at * IMA Game Theory Conference * in Oxford * 10 - 12 December 2014

A Resilient MAC Protocol for Wireless Networks

Jacob Abegunde, Hannan Xiao and Joseph Spring
School of Computer Science
University of Hertfordshire UK

Abstract

The IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN). The protocol was designed with the implicit assumptions that nodes would always follow the protocol rules and regulations. There was no provision to check for compliance with these rules, neither was there any provision to enforce such compliance. Consequently, for selfish or malicious reasons, nodes may choose to deviate from these specifications leading to misbehaviour and denial of service in the MAC layer. This paper briefly examine the existing solutions to the problem and provides a proposal for a resilient solution, using the concept of game theory.

Keywords: *MAC protocol, security, game theory, adversarial collaboration*

1. Introduction

The use of wireless network is gradually shifting from convenience to mission critical. This has led to exposure of various forms of vulnerabilities in the IEEE 802.11 wireless MAC protocol. The exploitation of these vulnerabilities has resulted in varieties of cheating and misbehaviour techniques, with denial of service (DoS) as the end product. This problem has been addressed by many researchers, but it still remains unsolved [1, 3, 7, 12, 20]. A large number of the proposed solutions centred around prevention, detection and reaction. A more resilient approach, we believe, is a proactive one in which node or user misbehaviour are considered as inevitable and so our aim is neither to prevent them nor to eliminate them but to incorporate mechanisms into the MAC protocol that will adapt it to various forms of misbehaviour so as to maintain a firm stance against them. This paper is divided into 5 sections. Section 1 deals with preliminaries and introduction. It serves as an introduction to the subject matter. Section 2 deals with game theory as a solution tool. In Section 3, the IEEE 802.11 MAC protocol misbehaviour problem, its scope, and previous solutions are discussed. Our proposal for resilient solution is discussed in section 4, while Section 5 is the conclusion of the study.

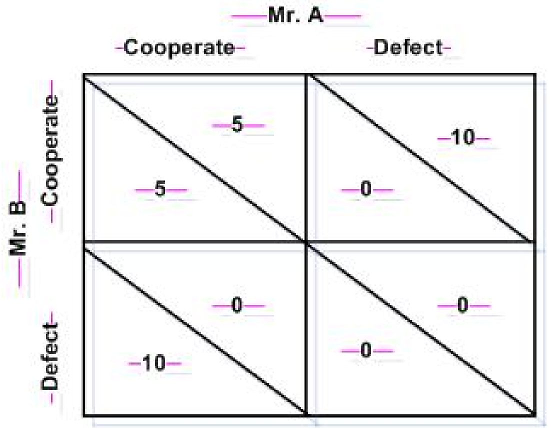
2. Basic Game Theory

Game theory is a multi-player decision theory. The players of a game are subjects that make the decision. The players participate in a game in order to get maximum benefit by selecting reasonable best actions. Thus the elements of a game includes players, information, strategy space and payoff or utility functions [26]. Game theory is a powerful tool for the study of situations of conflict and cooperation, and is concerned with finding the best actions for individual decision makers (i.e., players) in these situations that will lead to stable outcomes.

Suppose Mr. X has just graduated from a university with a first class degree in software engineering and has a novel idea of developing a mobile application that will enable users to drive and control their car using their mobile phone. If he needs to approach Mr. Y for finance, then there is a need for caution on both sides. Y may reasons thus: X has no track record of software development (unlike Google or Microsoft) and may just be a playboy. On the other hand, X may reasons thus: Y may take over the intellectual property and ownership of the business because of his financial involvement. And so a game has started already with both parties trying to minimize any risk that may be associated with such an agreement and also maximize their benefits, which is referred to as utility in game terms.

Similarly if two individuals, say Mr. A and Mr. B mutually agreed on a barter trade (BT) to exchange goods for goods and both of them are satisfied with the amounts of goods to be exchanged. Suppose for some reason, the trade must take place in secret with each of them leaving his bag at a designated place, say in a forest, and to pick up the other's bag at another designated place. Suppose it is clear to both of them that they may never meet or have further dealings with each other again. Then clearly, there is something to be afraid of, namely: the other person may leave an empty bag.

Obviously, if they both leave a full bag as previously agreed, they will both be satisfied, but equally obvious is the fact that, getting something for nothing is even more 'satisfying' and 'rewarding' (from a selfish behaviour perspective). So there is a tendency that both of them will be tempted to leave an empty bag. In fact, Mr. A can reason it thoroughly and rigorously in this manner: 'If Mr. B leaves a full bag as agreed, I will be better off having left an empty bag, because I would have gotten all that I wanted and given nothing away. On the other hand, if he decided to play smarter and clever than me and leaves an empty bag, thinking that I will leave a full bag, I will still be better off having left an empty bag, because I wouldn't be cheated. I will gain nothing but lose nothing either, which is good. Therefore, no matter what Mr. B chooses to do, I am better off leaving an empty bag. So I will definitely leave an empty bag'.



		Mr. A	
		Cooperate	Defect
Mr. B	Cooperate	5 5	10 0
	Defect	0 10	0 0

Table 1: BT Matrix Table

Meanwhile, Mr. B, being in more or less the same situation at the other end, will have similar thought and reasoning and thus arrives at the same parallel conclusion that his best strategy is to leave an empty bag. And so both of them, with their sophisticated and rational logic which seems infallible, will leave empty bags, and return home with empty bags. This is a practical example of a prison dilemma game and it illustrates how players' rationality could lead to suboptimal results in game theory. If we denote the strategy or action of leaving a full bag by cooperate (C) and that of leaving an empty bag (selfish behaviour) as defect (D), then the matrix table for this barter game is as shown in Table 1 below in terms of the player payoffs. A payoff of 5 signifies maximum utility while a payoff of zero signifies no utility. As discussed above, the best response strategy for Mr. A and B is to defect regardless of what strategy the other person might play. In game theoretic terms, we say defect is the dominant strategy. Now, how can we resolve such dilemmas? If the relationship between the players is to be sustained over a period of time and the game is to be repeated several times, then the prospect of future cooperation and future retaliation may keep both players from finking (i.e defecting). In order words, the prospect of future cooperation and future retaliation will influence the strategy of play. It will motivate player to cooperate during the early moves of the game and to defect towards the end of the game. This is an illustration of Tit-For-Tat (TFT) strategy in solving non-cooperative games.

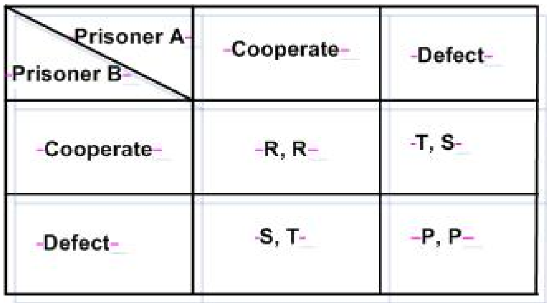
Games may generally be categorized as non-cooperative or cooperative. A non-cooperative game is concerned with the analysis of strategic choices and explicit models for the decision making process of a player out of its own interests. In cooperative games the players can make binding commitments. It is a game where groups of players ("coalitions") may enforce cooperative behaviour, hence the game is a competition between coalitions of players, rather than between individual players [24]. According to whether the movement of the players are simultaneous or not, non-cooperative games can be categorized as static or dynamic games. In a static game, players make their choice of strategies simultaneously, without any knowledge of what the other players will choose, whereas in a dynamic game there is a strict order of play. Players take turns to make their moves, and they know the previous moves of other players and can take that into consideration when choosing their strategy of play [21].

2.1 Prisoner's Dilemma (PD) Game

An understanding of the Prisoner's Dilemma or its variants is useful in appreciating the decision of whether to compete with rivals, or collude with them, whether to oppose and resist them or simply cooperate with them. In order to illustrate the kind of difficulties that may arise between two-person or groups in non-cooperative variable-sum games, the Prisoners Dilemma (PD) game, was originally formulated by a Canadian mathematician, Albert W. Tucker [4, 22]. It goes as follows:

Two prisoners, A and B, suspected of committing a bank robbery together, were isolated and urged to decide simultaneously whether they want to cooperate or defect, i.e each must decide whether or not to confess without knowing his partners' decision. Both prisoners, however, were told the consequences of their decisions as follows:

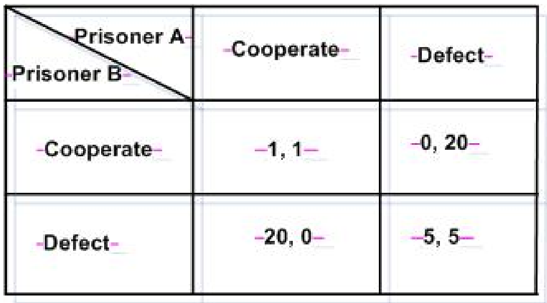
- if both confess, refer to as 'defect' (D), both go to jail for five years known as the 'punishment' payoff, P (for bank robbery).
- if neither of them confesses (i. e say nothing to the police), refer to as Cooperate (C) with each other; both go to jail for one year as 'reward' payoff (R) (for carrying concealed weapons since there is insufficient evidence for a robbery conviction).
- if one confesses, i.e defect (D), while the other cooperate (C) by keeping quite, the confessor goes free for confessing (defecting) and the silent one receives a 20 years jail term for cooperating with his partner. The 20 years sentence of the cooperator is known as the 'sucker' payoff, S, while the defector's condition of 'getting off the hook'(i.e discharged and acquitted with zero jail term), is known as the 'temptation to defect' payoff, T.



Prisoner A Prisoner B	Cooperate	Defect
Cooperate	R, R	T, S
Defect	S, T	P, P

Table 2: PD Matrix Table-A

The matrix table for the PD game is as shown in Table 2 and Table 3 in terms of payoff and jail terms. From this matrix table, T = 0, R = 1, P = 5, and S = 20. T>R>P>S. ('>' should be read or interpreted as 'better than', since the values actually represent the jail term in years) [4, 22].



Prisoner A Prisoner B	Cooperate	Defect
Cooperate	1, 1	0, 20
Defect	20, 0	5, 5

Table 3: PD Matrix Table-B

The explanation of PD is as follows: Though Prisoner A cannot be sure of what Prisoner B will do, (even if they had previously agreed on what to do) he knows that, it is better for him to confess, when B confesses (he gets 5 years rather than 20) and also when B remains silent (he serves zero term rather than a year) and B will similarly reach the same conclusion. So the solution would seem to be that, it is better for each prisoner to confess regardless of what the other may do and consequently they will both confess (Defect) and go to jail for five year each. Therefore Defection (D) is the dominant strategy.

Paradoxically, however, the two robbers would have done better if they both adopted the apparently irrational strategy of cooperating (C) with each other by keeping quite, since each would then serve only one year in jail. The real dilemma in this PD game is that, when each of the two (or more) parties acts selfishly and refuse to cooperate with one another, they do worse than when they act unselfishly and cooperate with one another.

The dilemma arise as a result of the fact that although mutual cooperation yields the highest collective payoff of 1 for each of the two players, individual defectors will do better with payoff zero, if the opponent decides to cooperate. Since selfish players are aware of this fact, both will defect, meaning none of them gets the much desired zero payoff. Thus, instead of them sharing the rewarding collective payoff of 1 that would have been received by mutual cooperation, they both end up worse off, with a payoff 5 received as a result of their individual defection.

The precarious situation of these 2 robbers will, hopefully, not be applicable to most of us, however, they are not the only one in this kind of dilemma. The dilemma applies to business strategists who may want to outdo their rivals, and the superpower nations of the world that engage in arms races [4]. It also applies to international trade, politics, economic decision and military strategies and engagement as well as well as war against terrorism. It cuts across every areas of life, which is why the security protocol developers and the protocol attackers are facing this same dilemma [25].

Adversarial collaboration i.e cooperating with an enemy is not a new concept. One of the early examples of the concept was proposed by Daniel Kahneman, for two researchers advocating competing hypotheses to collaborate on a research project with the goal of resolving their differences. It was based on the assumption that this would be more productive than when they are at odds with each other with each researcher conducting their own experiments individually and publishing conflicting responses to each others' papers [2]. Adversarial collaboration requires that people with opposing goals come to agreement, usually producing a shared product that reflects the interests of the adversarial parties. This is why it applies to the conflict between protocol developers and protocol breakers. However, adversarial collaboration is not the answer to all conflict scenarios and whenever it fails to yield the desire result, Tit-For-Tat (TFT) becomes the prominent strategy of play. With this little exploration of basic Game theory, we will now proceed to its application in MAC protocol security.

3. MAC Protocol Misbehaviour

3.1 The Problem

It has been observed that security threats to wireless networks are increasing and has accounted for an increase in MAC layer misbehaviour due to selfish or malicious reasons, significantly degrading the performance of wireless networks [3]. A selfish or greedy node typically misbehaves to improve its own performance at the expense of the other nodes. For instance a selfish node in a wireless sensory network (WSN) may refuse to forward packets on behalf of other hosts in order to conserve its energy [19].

A greedy host may exploit the vulnerabilities in IEEE 802.11 MAC protocol to increase its share of bandwidth. For example, IEEE 802.11 MAC protocol requires nodes competing for the channel to wait for a back-off interval before transmissions after it observes or experiences a collision. However, a selfish node may deliberately choose to wait for a smaller back-off interval, thereby increasing its chance of accessing the channel and hence increasing its shared throughput at the expense of well-behaved nodes or users [17].

Similarly, with the implementation of the MAC protocol in software rather than hardware or firmware on Network Interface Cards (NIC), it is easy to modify the protocol for misbehaviour as discussed in [16]. A change in protocol parameters in one or a set of nodes can have a devastating effect on the overall network performance which could lead to Denial of Service (DoS). While a well-behaved node strictly obeys the pre-defined protocol rules, the misbehaving nodes may deviate from the standard to either cause unfairness problems or disrupt the network services [19] A misbehaving node may keep on sending packets in order to reduce the chance of another node with lighter load to transmit, thereby monopolizing the medium. In a WSN, a node may send large amount of packets to a specific victim for forwarding (with the victim being a forwarding node) thus draining out the energy of the victim [16].

Two nodes may also collude with each other to establish a flow with continuous data transmission as discussed in [30], which can deplete the channel's capacity to transmit any other data. A selfish node may adjust its back-off interval in different ways to access the channel with higher probability of success as explained in [16]. One example of this is to choose a small back-off value rather than a valid generated random number by the back-off algorithm, e.g., using range [0,CW/2] rather than [0,CW] (where CW signifies contention window) or by generating a small random value regardless of the range. In the event of a collision or a busy medium, a selfish node will have a higher chance of winning the channel than any other nodes [16].

A selfish node may also set longer time duration than the actual transmission time in its Ready To Send (RTS) or Clear To Send (CTS) or DATA frames. Since the neighbour nodes that overhear such messages are not aware of the 'deception', they will adjust their Network Allocation Vector (NAV) according to the received messages and consequently defer longer time before transmitting [16]. A node can also adjust the Distributed Coordinated Function Inter Frame Space (DIFS) or Short Inter-frame Space (SIFS) time (by selecting smaller values) to further exacerbate the unfairness [18]. So while selfish behaviour include misbehaviour techniques such as the manipulation of protocol parameters like CW, NAV and DIFS etc, to take advantage of the weakness in the protocol design mechanism, malicious behaviour, on the other hand, aims at disrupting network devices or services, such as intentionally dropping MAC frames RTS/DATA [18]. All these evidence points to only one thing: IEEE 802.11 MAC protocol is vulnerable. These vulnerabilities have imposed additional constraint in the design of a new wireless MAC protocol.

3.2 The Previous Solutions

The various proposed solutions can be categorized as shown in Figure 1

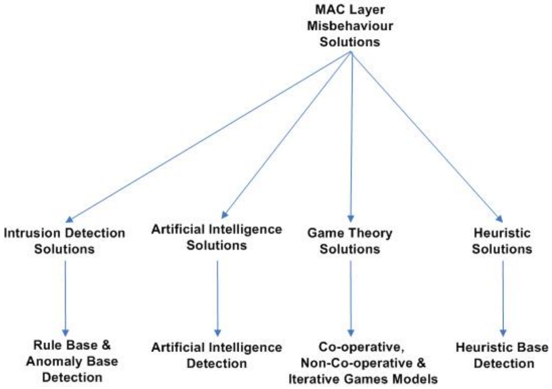

MAC Layer Misbehaviour Solutions
Intrusion Detection Solutions
Artificial Intelligence Solutions
Game Theory Solutions
Heuristic Solutions
Rule Base & Anomaly Base Detection
Artificial Intelligence Detection
Co-operative, Non-Co-operative & Iterative Games Models
Heuristic Base Detection

Figure 1: MAC Layer Misbehaviour Solutions

- **The intrusion detection approach** is based on developing a long-term profile of normal activities and identify misbehaviour and intrusion by observing deviations from the measured profile. The profiling process may involves data mining, clustering, machine learning, etc. These methods, though viable will introduce a long delay in the detection process in addition to their false positive. [13].

- **The game theoretic solution** based on the mathematical model of conflicts and resolution [14, 23] is another prominent method that has been used by researchers. A game could be cooperative or non-cooperative with each player trying to maximize its utility, but whether it is a cooperative or non-cooperative game, it usually involves a fundamental assumptions of rationality and/or perfect knowledge of players which may not be true in all situations and so may need some modifications in order to make it a practical solution.

- **The artificial immune system approach** is based on principles adapted from the Human immune system (HIS) and in some way similar to the intrusion detection method. The basic ability of HIS is an efficient detection of potentially harmful foreign agents (like viruses and bacteria). Likewise, the goal of AIS, is the identification of nodes with behaviour that could possibly negatively impact the stated mission of the wireless network [10, 11]. Like most methods of anomaly detection, the learning period required to identify what is 'normal' is a challenge in this method, in spite of the low computation overhead attributed to the method.
- **The heuristic approach** is based on systematic evaluation of communication parameters to detect misbehaviour and then allocate punishment scheme to serve as deterrent to the misbehaving node. The detection technique could be probability based and/or involve deviation from known rules. This heuristic approach refers to experience-based techniques for problem solving, that give a satisfactory solution though it may not be optimal. This method has been successfully used by various researchers in [6, 9, 15].

3.3 The Motivation

In spite of the wholesome benefits of wireless networks, some organizations are still very reluctant in deploying them into widespread usage as a result of these security concerns. However, as these security issues are being addressed, Wireless LAN is gradually becoming increasingly popular to the point that some organization staff are prepared to stick a rogue access point under their desk in the office to provide themselves with the much desired wireless connection even when their organization security policy clearly forbids such practice. This is an indication of the potential that lies ahead of the wireless network if only it could be made more secure.

In a time frame of just six months, there has been a massive roll out of wireless networks in my organization, the University of Hertfordshire. This is still ongoing and the target is to have an access point in every 20 square metre or one access point to 10 users, given that each user has a minimum of two wireless nodes: a mobile phone and a laptop. Others may have IPAD, Kindle and other portable wireless devices. This becomes very significant when considering a population of more than 30,000 users in my organization, as does the task of securing such a number of mobile nodes. Therefore, We believe that enhancing the MAC protocol with a resilience feature to ensure that it's capable of self-defence without any human intervention is the best way to go.

Another dimension to this problem of MAC protocol security is that there are dubious manufacturers and vendors who may implement any of the cheating techniques as discussed in section 3.1 above or a combination of them on their wireless Network Interface Card (NIC) to violate wireless MAC protocol rules in order to bring about a performance enhancement of their products for marketing or sales advantage [27]. The most prominent effect of this manufacturer or vendor factor is the fact that it makes a node or a user misbehave without being aware of it. This because in most cases, an innocent user who purchases a wireless device, does not, in general, bother about the implementation of the IEEE 802.11 MAC protocol in such device, so the user may use such a device in ignorance of the hazards it constitutes to other nodes or users. Such a user may eventually take down the wireless network unknowingly and cause a denial of service. Thus, the motivation behind this study is the desire to improve wireless network security, not only to simplify the job of security management, but to make the wireless MAC protocol resilient to misbehaviour by responding adaptively.

4. The Resilient MAC Protocol

4.1 The Overview

According to Wikipedia, the word robust, when used with regard to computer software, refers to an operating system or other program that performs well not only under ordinary conditions but also under unusual conditions that stress its designers' assumptions. Robustness has to do with maintenance of functionalities of the system against all odds. It does this by avoiding or preventing failure, but its performance may suffer in the process.

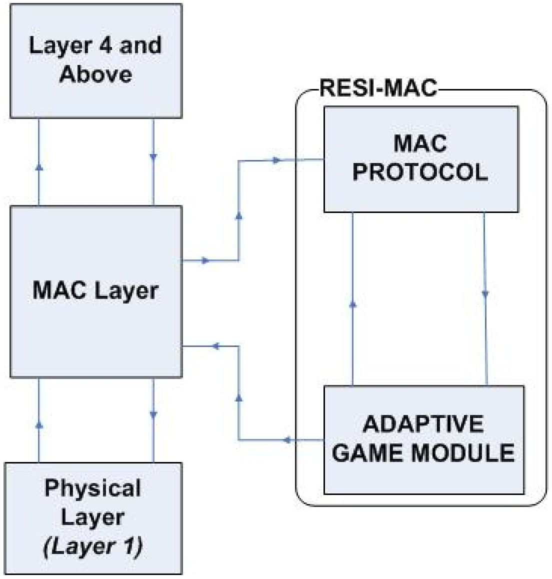


Figure 2: Resilient MAC Protocol

On the other hand, a system is resilient when it can adapt to internal and external challenges by changing its method of operations while it continues to perform its function. And so, resilience represents the capacity of a system to anticipate and manage risk effectively, through appropriate adaptation to its functionalities. In order words, the resilience approach reacts intelligently to adverse situations by neutralizing their effect. So while a robust strategy says: 'misbehaviour should not stop the functionality' (i.e the focus is on maintaining functionality against all odds without any fundamental changes to the original system), a resilient strategy says: 'misbehaviour should be neutralized or managed by changing the operational mode' (i.e the focus is on adaptation to odds situations through a fundamental shift or change in mode of operations).

The IEEE 802.11 MAC protocol in its original state is an example of a robust system. It keeps on working, though with some decline in performance, in the event of misbehaviour activities. It has no mechanism in place to change its operational mode in the event of misbehaviour and so it may struggle hard to keep working. However, a resilient based approach will react intelligently by changing its operational mode so as to adapt itself to misbehaviour by working in a strategic mode while the misbehaviour activity is ongoing, and switching back to the normal operational mode when the misbehaviour activity ceased. In essence, a resilient approach acknowledges the potential for misbehaviour (i.e deviation from the rules) and focuses on adapting to it rather than assuming that all nodes will follow the rules of engagement.

In our approach, a resilient MAC protocol is a non-cooperative game in which adversarial collaboration would have been the best solution option, however because it is very risky to trust an adversary even after they have agreed to cooperate, there is a need to technically enforce co-operation by providing a negative incentive associated with the protocol misbehaviour. The original MAC protocol encourages cooperation by stating the rule, but then it leaves players to decide whether to obey the rule or not. There is no disincentive for misbehaviour. Those who misbehave do so as a result of greediness to gain more bandwidth, or some other performance enhancement at the expense of other normal users and in the process cause a DoS. So, in our approach we acknowledge that the MAC protocol will sometimes be subjected to nodes' manipulation and misbehaviour, and hence make provision for such scenario in advance by incorporating an adaptive game module into the protocol as shown in Figure 2, to adapt the protocol to misbehaviour when necessary. This is the idea behind the proposed resilient MAC protocol.

4.2 The DCF MAC Game Model

In order to provide a game theoretic solution to the problem of misbehaviour in Wireless LAN (WLAN), we first analyse the operation of the IEEE 802.11 DCF MAC from game theory perspective and the interaction between players (nodes) using static game concept. As explained earlier, a static game is one in which all players make decisions (or select a strategy) simultaneously without the knowledge of the strategies that are being chosen by other players. In our DCF game, each player (node) has two actions space: Transmit or Not transmit (i.e., Wait) and two strategies: Cooperate (C) or Defect (D) following from [8]. We then proceed to modelled the DCF as a non-cooperative game and in order to do this, we specify the following:

- **the set of Players**
- **the set of Strategies**
- **the set of Utilities**

Therefore our MAC game can be formulated as as a 3-tuple:

$G =< N_i, S_i, U_i >$

where

- N_i is the set of players (nodes).
- S_i is the strategies or action set of player i, $S = S_1 * S_2 * ...S_n$ which is the Cartesian product of the set of actions available to each player.
- U_i is a set of utility functions that each player i wishes to maximize.

4.3 Assumptions

In the application of game theoretic solution to the problem of misbehaviour in WLAN, one of the the generic assumptions is that of rationality of all nodes. This in a way means that nodes are interested in maximizing their own utilities alone. If we assume they do this regardless of the cost to other players (selfish behaviour), then we will end up with all of them being classified as selfish and thereby misbehaving nodes. This assumption has been criticized by many scholars [5] including ourselves simply because it labels all node as misbehaving which is a bit on the extreme side and difficult to justify. So we thought this assumption could be validated if modified to account for selfish (i.e misbehaving) nodes as well as normal nodes, both of which are players in any DCF game. This modification will result in changing the way in which MAC protocol game will be formulated and played and consequently the preferred solution to misbehaving nodes. Now, let us consider these two classes of nodes in a little bit of details. Misbehaving nodes are selfish nodes that try to maximize their own benefit or utility at the expense of the other nodes by disregarding the protocol rules. These misbehaving or selfish nodes are interested in their own welfare rather the common (social) welfare of all. On the other side of selfish and misbehaving nodes are good nodes that always cooperate and obey the protocol rules. We deliberately avoid the use of the word 'selfless' (the opposite of selfish) in referring to them as that will mean they are self sacrificing or doing something extra ordinary which is not what we mean and so we called them normal nodes, meaning they simply play by the rules. These normal nodes are also rational in the sense that they would want to maximize their expected utility, however not at all cost, that is, not at the expense of the common goal and common utility which differentiate them from the selfish node.

4.4 The Solution Concept

They are two major solution concepts for such non-cooperative games: one solution concept is to provide an equilibrium condition (NE) in which no player can increase its utility by unilaterally changing its strategy, a state known as Nash Equilibrium (NE). The other solution concept is to provides incentives to those players that behave properly by obeying the protocol rules and disincentives for nodes that disregard protocol rules for selfish reasons. The incentives can be in form of good reputation while disincentives can be in form of bad reputation or punishment scheme for misbehaviour

[8, 21, 27, 29]. The implementation of reward and punishment scheme always present some issues such as the requirement for a monitoring and detecting host. This could be implemented at Access Point (AP) or an independent device may be introduced as a watchdog. Whichever way it is implemented, this constitutes an additional load in the WLAN. In addition to this, there is no general consensus on the size of the reward and punishment, so each researcher implements what seems best to them. And finally on this, the scalability and adaptability of such solutions could be a challenge in the sense that the detection of misbehaviour techniques may lead to discovery of evasion techniques since security implementation is a hide-and-seek game. Our approach to solve this problem is to propose mechanisms which force the selfish nodes to follow the rules under the threat of retaliation. Hence, rational nodes (both selfish and normal) will be forced to cooperate, in order to maximize their expected payoff.

4.5 The DCF MAC Game Analysis

In order to present our game strategy and solution concept, we analysed the DCF game as a non-cooperative game in which each node makes independent decision of whether to obey or disobey the protocol rules based on personal motivations best known to them. As stated earlier for this DCF MAC game, the players choose their strategies autonomously and are not bound by any inter-player agreements except for self-enforceable one (i.e within their will). For the sake of simplicity, we consider a number of saturated nodes in the same transmission range: saturated in the sense that they always have packets to transmit and within the same transmission range in the sense that they can hear one another without any interference. In order to analyse our solution concept to the problem, we specify:

- Players as wireless nodes (both normal and misbehaving and selfish).
- Strategies space as: Cooperate (C) meaning obey the protocol rules and Defect (D) meaning disobey the protocol rules.
- Normal nodes comply with the standard protocol by using the specified CW and EBO parameters.
- Selfish nodes violate the protocol standard by doing the opposite for example maintaining a small fixed CW or small Exponential Back-Off (EBO) such as CW_{min}, $\frac{CW_{min}}{2}$, $\frac{EBO}{2}$ etc, which can be represented as $\frac{CW}{n}$ and $\frac{EBO}{n}; n \in \mathbb{Z}$.
- Utility refers to payoff or benefit (e.g. increase in performance or throughput gained) which we denote collectively as throughput.

For the sake of simplicity, let us limit the number of players (nodes) to 2 for now, the strategy space are as follows:

- CC when both of them cooperate and obey the protocol rules.
- CD when node 1 Corporates and node 2 Defects.
- DC when node 1 Defects and node 2 Corporates.
- DD when both players Defect.

Let us consider the different scenarios and their outcome as follows:

- Scenario 1: When both nodes cooperate (CC) by obeying the rule, the combined utility $U = U_{cc}$: The two nodes have an almost equal chance of accessing the channel. The probability of collision is minimized and throughput is shared almost equally and their combined Utility is increased.
- Scenario 2: When node 1 cooperates and node 2 defects CD: node 2 (unfairly) gets U_d, a higher part of the utility at the expense of node 1 who gets U_c.
- Scenario 3: When node 1 defects and node 2 cooperates DC: node 1 (unfairly) gets U_d, a higher part of the utility at the expense of node 2 who gets U_c.

- Scenario 4: When both nodes defect (DD) by disobeying the rule, the probability of collision increases considerably and the utility U_{dd} diminish for both nodes.

We can now illustrate these scenarios as a normal-form game where:

- Players (P)
- Nodes $N = \{1, 2\}$
- Strategies (Action): $S = \{C, D\}$
- Utilities Space for the 2 nodes (i.e Possible Payoffs): $U_s = \{U_{dd}, U_{cd}, U_{dc}, U_{cc}\}$

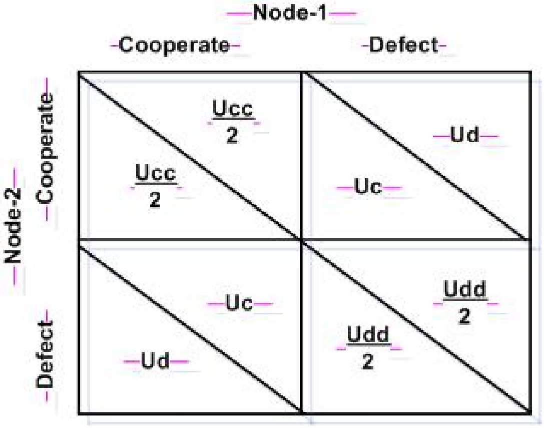
The game matrix table is as shown in Table 4.

Suppose that the combine utility for both nodes approaches zero for combine defection (DD) scenario and it approaches U_{max} (i.e maximum) for combine cooperation (CC) scenario, then $U_{dd} \to 0$ for a worst case scenario and $U_{cc} \to U_{max}$ for a best case scenario, so then, $U_s = \{0, U_{cd}, U_{dc}, U_{max}\}$; $\{0 < U_{cd/dc} < U_{max}\}$.

If node 1 is playing D, the best strategy choice for node 2 is to play D as well, playing C will not do it any good as it offers zero payoff. Similarly, if node 1 is playing C, the best choice for node 2 is to play D which is not socially optimal, but it offers a higher payoff for node 2. If both players commit to play the strategy C, they will be better off. The normal-form game is similar to the Prisoner's Dilemma with D as the dominant strategy over the C leading to suboptimal result.

It can be concluded that the CSMA/CA mechanism of DCF works well if all nodes follow the predefined rules, however, as observed above, violating the protocol promises greater rewards. Nodes do not have sufficient information on what the other nodes will do and so may play their best response (most rewarding) strategy. If they all decide to violate the protocol individually to get the grater rewards, the network performance may suffer leading to a phenomenon referred to as tragedy of the commons: a situation in which individuals, acting independently and rationally according to each one's self-interest, behave contrary to the whole group's long-term best interests [31].

So how can we stimulate cooperation and make the equilibrium Pareto Optimal and fair for the common good of all? This is where the Tit-For-Tat (TFT) strategy comes into play. Although TFT strategy has a deadlock vulnerability in its default mode, it can be used in modified form. In our earlier Barter Trade (BT) game, it is fairly obvious that the players' strategic decisions will depend on their likelihood of future encounters. If they know that they are destined never to meet again as we assumed, then defection is the only rational choice, both players will cheat and end up badly with little or no payoff as discussed. Similarly, the game between the ambitious graduate and his financier partner as discussed earlier is not any different: the chance of cooperation is slim if the relationship is going to be temporary.



		Node-1	
		Cooperate	Defect
Node-2	Cooperate	$\frac{Ucc}{2}$ $\frac{Ucc}{2}$	Ud Uc
	Defect	Uc Ud	$\frac{Udd}{2}$ $\frac{Udd}{2}$

Table 4: MAC Game Matrix Table

However, if these games are to be repeated over a number of times, then a selfish players will realised that, it is better to cooperate on the early moves and then cheat only towards the end of the game. In such an iterated game when players know the total number of iterations in advance, they do indeed cheat more often in the final lap. Consequently, all players tend to cooperate more when the number of iteration is either unknown or significantly large [28]. This is a demonstration of the effectiveness of TFT strategy in stimulation of cooperation in a non-cooperative game.

5. Conclusion

There is no guarantee that any nodes (users) will always obey the MAC protocol rules and so whether we like it or not WLAN user nodes population will always consist of both selfish (misbehaving) and good (normal) nodes. Therefore our aim is not to eliminate or stop selfish behaviour or misbehaviour, but to find a middle ground in which both the normal nodes and selfish nodes can co-exist without breaking the protocol. That is, a game in which both selfish and normal user can achieve a balanced payoff, Pareto efficiency or social welfare (i.e common good).

In order to achieve this, there is the need to first acknowledge the fact that the MAC protocol will sometimes be under attack or subjected to manipulation and node misbehaviour and then make provision for such scenarios in advance by incorporating a resilient module into the protocol stack as shown in Figure 2 to handle such odd situations whenever they arise so that the protocol can continue to work without little or no hindrance in hostile and adversarial condition.

This is the idea behind the proposed resilient MAC protocol. Since game theory offers ways to formulate and solve problems posed by players in a conflict or non-cooperative environment like the WLAN, it can serve as a favourable tool for analysis of the IEEE 802.11 DCF MAC protocol and in finding the optimal operating points in such an adversarial condition as discussed, so that the much preferred collaboration between primitive users and sophisticated adversaries can become technically feasible.

.

References

[1] Md Sohail Ahmad and Shashank Tadakamadla. Short paper: security evaluation of ieee 802.11 w specification. In *Proceedings of the fourth ACM conference on Wireless network security*, pages 53–58. ACM, 2011.

[2] Ian Bateman, Daniel Kahneman, Alistair Munro, Chris Starmer, and Robert Sugden. Testing competing models of loss aversion: An adversarial collaboration. *Journal of Public Economics*, 89(8):1561–1580, 2005.

[3] Kemal Bicakci and Bulent Tavli. Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks. *Computer Standards & Interfaces*, 31(5):931–941, 2009.

[4] Caoqian and Chen Jingliang. Discussion on role of credibility failure punishment cost in game between the government and the public 2014;model analysis based on prisoner dilemma. In *Information Science and Engineering (ICISE), 2010 2nd International Conference on*, pages 2771–2775, 2010.

[5] Lin Chen and J. Leneutre. Selfishness, not always a nightmare: Modeling selfish mac behaviors in wireless mobile ad hoc networks. In *Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on*, pages 16–16, June 2007.

[6] Jaehyuk Choi, A.W. Min, and K.G. Shin. A lightweight passive online detection method for pinpointing misbehavior in wlans. *Mobile Computing, IEEE Transactions on*, 10(12):1681–1693, 2011.

[7] Kevin Collins, Stefan Mangold, and G-M Muntean. Supporting mobile devices with wireless lan/man in large controlled environments. *Communications Magazine, IEEE*, 48(12):36–43, 2010.

[8] Tao Cui, Lijun Chen, and Steven H Low. A game-theoretic framework for medium access control. *Selected Areas in Communications, IEEE Journal on*, 26(7):1116–1127, 2008.

[9] S. Djahel, Zonghua Zhang, F. Nait-Abdesselam, and J. Murphy. Fast and efficient countermeasure for mac layer misbehavior in manets. *Wireless Communications Letters, IEEE*, 1(5):540–543, 2012.

[10] M. Drozda, S. Schaust, and H. Szczerbicka. Ais for misbehavior detection in wireless sensor networks: Performance and design principles. In *Evolutionary Computation, 2007. CEC 2007. IEEE Congress on*, pages 3719–3726, 2007.

[11] M. Drozda, S. Schaust, and H. Szczerbicka. Is ais based misbehavior detection suitable for wireless sensor networks? In *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, pages 3128–3133, 2007.

[12] M. Eian and S.F. Mjolsnes. A formal analysis of ieee 802.11w deadlock vulnerabilities. In *INFOCOM, 2012 Proceedings IEEE*, pages 918–926, 2012.

[13] Alexandros G Fragkiadakis, Vasilios A Siris, and Nikolaos Petroulakis. Anomaly-based intrusion detection algorithms for wireless networks. In *Wired/Wireless Internet Communications*, pages 192–203. Springer, 2010.

[14] Antoniy Ganchev, Lata Narayanan, and Sunil Shende. Games to induce specified equilibria. *Theoretical Computer Science*, 409(3):341–350, 2008.

[15] V.R. Giri and N. Jaggi. Mac layer misbehavior effectiveness and collective aggressive reaction approach. In *Sarnoff Symposium, 2010 IEEE*, pages 1–5, 2010.

[16] Lei Guang and Chadi Assi. Vulnerabilities of ad hoc network routing protocols to mac misbehavior. In *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on*, volume 3, pages 146–153. IEEE, 2005.

[17] Lei Guang, Chadi Assi, and Abderrahim Benslimane. Mac layer misbehavior in wireless networks: challenges and solutions. *Wireless Communications, IEEE*, 15(4):6–14, 2008.

[18] Lei Guang, Chadi Assi, and Yinghua Ye. Dream: A system for detection and reaction against mac layer misbehavior in ad hoc networks. *Computer communications*, 30(8):1841–1853, 2007.

[19] R. Gunasekaran, V.R. Uthariaraj, R. Sudharsan, S. Sujitha Priyadarshini, and U. Yamini. Detection and prevention of selfish and misbehaving nodes at mac layer in mobile ad hoc networks. In *Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on*, pages 001945–001948, 2008.

[20] G.R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X.P. Costa, and B. Walke. The ieee 802.11 universe. *Communications Magazine, IEEE*, 48(1):62–70, 2010.

[21] Tao Jing, Yunqing Yang, Yuan Le, Liran Ma, Wei Zhou, and Yan Huo. A multiple access game based mac protocol for fairness provisioning and throughput enhancement. In *Wireless Algorithms, Systems, and Applications*, pages 346–357. Springer, 2012.

[22] N. Kishimoto, S. Kokubo, and J. Tanimoto. Network reciprocity on spatial prisoner's dilemma games by continuous-binary strategy. In *Soft Computing and Intelligent Systems (SCIS) and 13th International Symposium on Advanced Intelligent Systems (ISIS), 2012 Joint 6th International Conference on*, pages 663–668, 2012.

[23] Jerzy Konorski. A game-theoretic study of csma/ca under a backoff attack. *IEEE/ACM Transactions on Networking (TON)*, 14(6):1167–1178, 2006.

[24] Chunfeng Liu, Yantai Shu, Wucheng Yang, and Oliver WW Yang. Performance analysis of ieee 802.11-based ad hoc networks using game theory. In *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*, pages 246–250. IEEE, 2008.

[25] R.T.B. Ma, V. Misra, and D. Rubenstein. Modeling and analysis of generalized slotted-aloha mac protocols in cooperative, competitive and adversarial environments. In *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on*, pages 62–62, 2006.

[26] SHE Mortazavi Najafabadi and CC Constantinou. Game theoretic approach to medium access control in wireless networks. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pages 872–877. IEEE, 2013.

[27] K. Piamrat. Punishment protocol for backoff manipulation in mac ieee 802.11. In *Communications and Information Technologies, 2006. ISCIT '06. International Symposium on*, pages 1013–1016, 2006.

[28] Debarshi Kumar Sanyal, Matangini Chattopadhyay, and Samiran Chattopadhyay. Performance improvement of wireless mac using non-cooperative games. In *Advances in Electrical Engineering and Computational Science*, pages 207–218. Springer, 2009.

[29] S. Shivshankar and A. Jamalipour. Effect of altruism and punishment on selfish behavior for cooperation in vehicular networks. In *Communications in China (ICCC), 2012 1st IEEE International Conference on*, pages 653–658, Aug 2012.

[30] Alberto Lopez Toledo and Xiaodong Wang. Robust detection of mac layer denial-of-service attacks in csma/ca wireless networks. *Information Forensics and Security, IEEE Transactions on*, 3(3):347–358, 2008.

[31] Bo Yang, Gang Feng, and Xinping Guan. Noncooperative random access game via pricing in ad hoc networks. In *Decision and Control, 2007 46th IEEE Conference on*, pages 5704–5709. IEEE, 2007.