A Dynamic Game with Adaptive Strategies For IEEE 802.15.4 and IoT

Jacob Abegunde
School of Computer Science
University Of Hertfordshire
Hatfield, UK AL10 9AB
Email:j.abegunde@herts.ac.uk

Hannan Xiao
School of Computer Science
University Of Hertfordshire
Hatfield, UK AL10 9AB
Email: h.xiao@herts.ac.uk

Joseph Spring
School of Computer Science
University Of Hertfordshire
Hatfield, UK AL10 9AB
Email: j.spring@herts.ac.uk

***Abstract*—The problem of selfishness and misbehaviour in wireless networks is well known, as are the associated solutions that have been proposed for it in IEEE 802.11 Wireless Local Area Network (WLAN) and Wireless Sensory Network (WSN). However, tackling such problem in relation to the Internet of Things (IoT) is relatively new since the IoT is still under development. The central communication infrastructure of IoT is the IEEE 802.15.4 standard which defines low-rate and low energy wireless personal area networks. In order to share the medium fairly and efficiently in a beacon-enabled mode, the standard uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in the Contention Access Period (CAP), and Guarantee Time Slot (GTS) in the Contention Free Period (CFP) of a super-frame. These channel sharing mechanisms are known to be vulnerable to selfishness, misbehaviour and channel capture as a result of nodes disobeying the communication rules. Most of the existing game theoretic solutions were designed for IEEE 802.11 WLAN and WSN. In this work, we present a dynamic game in which nodes can select and adapt their strategies of play according to the 'state of the game' and their energy level in order to increase their utility whenever their utility declined. Our model enables resources constrained nodes to optimised their strategies individually based upon the current state of the game and their available resources. Our analysis and simulation results suggest an improvement in utility, and fairness in channel sharing, as well as efficiency in energy usage in our dynamic model and hence performance and security in our scheme over the default IEEE 802.15.4 access mechanism.**

***Keywords*—IEEE 802.15.4; IoT; Security; Game Theory;**

I. Introduction

Nearly everything goes by the name 'smart' these days. We have smart phones, smart homes, smart cars, smart cities, smart classrooms, and so forth. These are all indicative of IoT. One of the most significant product of network globalization effort is the IEEE 802.15.4 standard. It is widely recognized as one of enabling technologies for short range, low rate, wireless communications that is most suitable for IoT. As an effort towards the vision of a network globalization employing the loT, the global operation of plug and play smart devices in IPv6 networks has been proposed [1].

In order for the concept of IoT to be realised, every device in homes, industries, schools, and the environment will need to have a means of communication embedded into them in form of Radio Frequency Identifier (RFID) through which they can communicate and share data with other devices around them. In line with energy and environment consideration, there is a requirement for each device to participate in ultra-low complexity, ultra-low cost, ultra-low power consumption, and low data Wireless Personal Area Network (WPAN). This make the IEEE 802.15.4 standard a suitable candidate for IoT. Therefore, as we move towards the widespread implementation of IoT, it follows that the use of IEEE 802.15.4 standard is likely to increase as suggested by authors of [2] and [3].

However, as discussed in [2] and [4], the anticipated potential privacy and security risks of seamlessly connected devices in IoT has put a burden on stakeholders such as the IEEE and IETF, to provides solutions that address the problem. The inherent risk in machine to machine (M2M) communication, as a result of vulnerabilities in protocol design can impede the implementation of IoT. In order to overcome such impediments, the stakeholders: the IEEE, the IETF, the networking organisations, and the research community have proposed various security solutions for wireless communication.

For example, the use of symmetric-key cryptography techniques has been proposed to protect the IEEE 802.15.4 MAC specification and prevent spoofing. However the details of how to handle the initialization of a secure communication in IEEE 802.15.4 domain, the generation and the exchange of keys, and the management of joining operations in a secure IEEE 802.15.4 network are works in progress at the moment as discussed in [2] and [4]. Most of the proposed mechanisms are not yet implemented or tested, which means their potency and sustainability still remain unknown. At the moment, the IoT is a work in progress and so some of the mechanisms that will drive it are being put together, hence the extension of our work in [5] to this area.

Wireless networks are dynamic environments, designed to be cooperative with all nodes complying with a given set of rules. However, such rules are not being enforced and hence there is no guarantee that nodes will comply with the rules. In a dynamic environment, the behaviour of nodes could change from good to bad as a result of non-compliance with the rules, which could eventually lead to a Denial of Service (DoS).

With the on-going development of IoT and its applications, the security of wireless network is of increasing concern, with tackling misbehaviour a matter of priority for stakeholders of wireless networks. Several game theoretic models have been

proposed as solutions to misbehaviour problems in wireless networks. These solutions either incentivise good behaviour with good reputation, or dis-incentivise bad behaviour through punishment schemes, however in most cases, the application of these solutions are limited to IEEE 802.11 - WLAN and WSN.

The IEEE 802.15.4 is the building blocks and central communication infrastructure for IoT. Consequently, in this paper, we redesign our previous solution in [5] which is for IEEE 802.11, and modify it for IEEE 802.15.4 - IoT, by modelling the IEEE 802.15.4 MAC protocol as a non-cooperative dynamic game with adaptive strategies. Our model enables resource constrained nodes to evaluate the state of the game and their energy level and to select appropriate strategies for better utility, as a response to misbehaviour of other nodes. To the best of our knowledge, this is a new idea and it needs further exploration.

The rest of this paper is structured as follows: we discussed the relevant literature in section 2. Our proposal and model are discussed in section 3 while the analysis and evaluation are discussed in section 4, and finally, our conclusion and future works are discussed in section 5.

II. Relevant Literature

A. Related Work

In [3] and [6], the authors discussed the IEEE 802.15.4 as the wireless communications stack the industry believes to meet the important criteria of power-efficiency, reliability and Internet connectivity that is necessary for IoT, however, they also acknowledge the security issues, which they claimed could be taken care of at upper layer. The author of [7], in their write up, discussed greedy behaviours as one of the most aggressive DoS attacks in wireless networks, in which a compromised node consume the bandwidth at the expenses of other nodes by not respecting the access procedure. In their work, they proposed a solution to greedy behaviour which involves modelling Time Petri nets for sane and greedy nodes.

The work in [1] and [2] discussed the security challenge of IEEE 802.15.4 in the context of IoT, while the author of [8] discussed how GTS management schemes built-in security mechanisms still leave the IEEE 802.15.4 MAC vulnerable to attacks. They explained how the existing techniques in the literature for securing IEEE 802.15.4 cannot defend against insider attacks for beacon-enabled mode of IEEE 802.15.4.

In [6] the authors discussed how security competes with performance for the scarce resources in a low power, low cost sensor devices of IEEE 802.15.4 standard. They also evaluate the impact of security related operation on memory usage, network performance, and energy usage in IEEE 802.15.4 standard. However, contrary to this view in [6], the authors of [9] demonstrated that, for practical applications and implementations, security features introduce a negligible degradation that is often acceptable even for the most energy stringent systems. This apparent contradiction of research results further affirms that the subject of IoT and its foundation blocks, IEEE 802.15.4 is still in the infancy and experimental stage.

B. Research Gap

While the work in [5], [10], [11] and many others proposed game theoretic solutions to the problems of misbehaviour and selfishness in wireless networks, these works are mainly designed for IEEE 802.11 WLAN and WSN. On the other hand, the work in [1] and [12] discussed the vulnerability and security challenges in IEEE 802.15.4 and IoT. However, they do not address misbehaviour and selfishness in the standard.

Furthermore, [1] and [2] are survey works, highlighting the security problems in IEEE 802.15.4 and IoT for discussion and solutions. While a number of work such as [7] and [2] did proposed some solutions, such solutions are not game related and so they are significantly different from our work.

The difference between our work in [5] and this one is that the work in [5] was designed for IEEE 802.11 while this one is designed for IEEE 802.15.4. The communication mechanism of IEEE 802.11 differs from IEEE 802.15.4 and hence their solutions differs. Another major difference between the two solutions is that this solution is energy aware in the sense that the setting of contention window in a misbehaviour scenario is dependent on the available energy of the node, while the solution in [5] does not take available energy into consideration.

The IoT consist of three layers architecture: Perception, Network, and Application layers in which various security features can be implemented. Since there is no one method that fits all, a number of security suites such as data encryption, frame integrity, sequential freshness, data verification and access control which are conventional security suites are being implemented at different layers in order to achieve the principle of defence in depth. However none of these suites address misbehaviour at MAC layer hence they are different from our work.

C. Research Contribution

In this work, our main contributions is the modelling of IEEE 802.15.4 as a dynamic game. In our dynamic game, we modelled nodes as the players, with the capability to evaluate the state of the game and then modify their contention parameters in order to improve their utility in a misbehaviour scenario. The dynamic MAC model defaults to the standard IEEE 802.15.4 under normal condition. The state of the game refers to the number of transmission failure or Clear Channel Assessment (CCA) failure the node has suffered. In addition, our model enables resources constrained nodes to select their strategies of play individually and independently, based on the amount of energy available to them, thus making our model to be energy-aware and energy efficient.

D. The IEEE 802.15.4 Protocol

The focus of IEEE 802.15.4 standard is to provide short-range wireless links, low data rate WPAN with lower quality of service requirement, low complexity and low power consumption, unlike the IEEE 802.11 WLAN and WSN which has a throughput of 5.4M and often regarded as a 'heavy duty' protocol. The low rate WPAN IEEE 802.15.4 MAC is

responsible for a number of tasks ranging from association and disassociation, to periodic beacon transmission and communication synchronization to the actual channel access mechanism. The standard support star configuration as well as peer-to-peer topology. The transmission mode could be beacon-enabled or beacon-less, while the channel access method could be contention-based (unslotted CSMA-CA), contention-free (guaranteed time slots, GTS) or scheduled contention-based (slotted CSMA-CA).

This flexible configuration options together with low energy requirement makes it a well adapted standard for M2M communication. The data service allows the transfer of MAC Service Data Unit (MSDU) to a peer device, which may include an Acknowledgement (ACK) from the peer device and / or several retransmissions. The management service is responsible for device configuration, periodic transmission of, and synchronizing to beacons, enabling Personal Area Network (PAN) association and disassociation, employing security mechanisms and handling the GTS mechanism. The PAN usually has one coordinator - PAN Coordinator (PANC), a device which is the primary controller responsible for PAN identifier, device address assignment and device synchronization as discussed in [3] and [2].

In a beacon-less mode, frames are transmitted according to an unslotted CSMA-CA algorithm (non-persistent CSMA). If the channel is detected idle the transmission can start immediately otherwise the device waits for a random time period uniformly drawn from an exponentially increasing back-off interval. In beacon-enabled mode, the PANC periodically transmit beacons which mark the beginning or end of a super-frame. A beacon carries information about pending data and the current network configuration. It precedes CAP and ends the Inactive Periods (IP) in a super-frame. During the CAP, devices use a slotted variant of the CSMA-CA algorithm in which a device must sense an idle channel twice before it may transmit and both channel sensing and transmission must be performed on a back-off slot boundaries. The flexibility of this beacon enable mode makes it adaptable for Real Time Traffic (RTT) and Non-Real Time Traffic (NRTT) as observed in [3] and [2], hence the focus of this study is on the beacon enable mode only.

Fig. 1 shows the structure of a super-frame for the beacon enabled mode. It begins with a beacon, next to the CAP. The CAP is followed by an optional CFP, which is portioned into GTS slots. The GTS slots are allocated dynamically and the corresponding time interval can be used exclusively to transmit packets in a contention-free fashion. The CFP is followed by an optional Inactive Period (IP) in which all nodes can sleep to preserve energy and achieve low duty cycles.

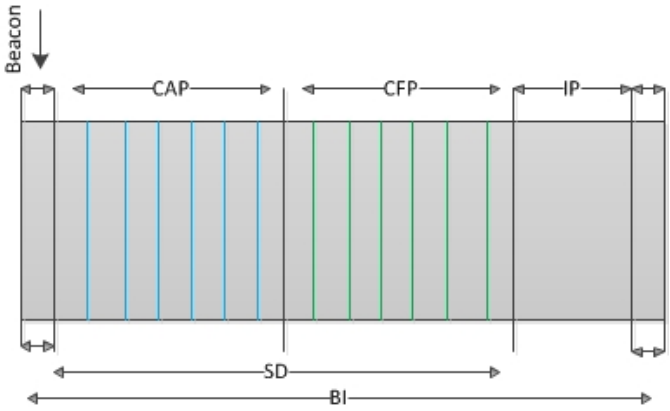

Fig. 1: IEEE 802.15.4 Super-frame Structure

III. The Proposed Model

A. Model Assumptions

In order to discuss our game with clarity, the following assumptions were made:

- Channel and traffic: We consider a single-cell wireless WPAN, with an ideal channel of negligible transmission error i.e. the network is noise free, meaning packet loss is only due to collision.
- Players: We suppose k nodes out of the n nodes are selfish and so defect by deliberately deviating from the IEEE 802.15.4 MAC protocol specification, while $(n-k)$ nodes cooperate and obey the rules. In this scenario, both k selfish nodes and $(n-k)$ normal nodes are players in the game. We considered all nodes rational, so that their objective is to maximize their utilities: individual throughputs per energy used in this case. We assume the nodes are all saturated with packets in order to maximise the channel usage, i.e. they always have packets to transmit and so the channel will operate at full capacity.
- Utility: We describe the utility or payoff of a player as its revenue derived from transmission of data which we denote as the throughput T (in mbps) per energy used E_u in (joules).
- Cost: We refer to the cost of transmission which is express as energy used E_u (in joules) per data transmitted - throughput (in mbps).
- Strategy: We also describe the strategy of each node i in terms of the selection of its contention parameters value subject to the other $n-1$ nodes such that the player's utility U_i, is maximized. That is, since our utility is expressed as T/E_u, then given the available energy E_a, each node strategy is to maximise T/E_a, i.e. using the E_a, in a way such as to get the maximum value for the ratio T/E_u. The E_a will be used to acquire U_i and hence E_a will turn to E_u after usage.

B. IoT Game States Transition

In order to discuss the dynamism of our game, let us start with the simplest mode which is a single stage game involving the process of sending a packet from source node to destination node using the state transition diagram in Fig. 2. The term $busy$ denotes that the channel is in use while $idle$ denotes that it is free for use. The state transition and the channel access mechanism for both CAP and GTS are discussed below.

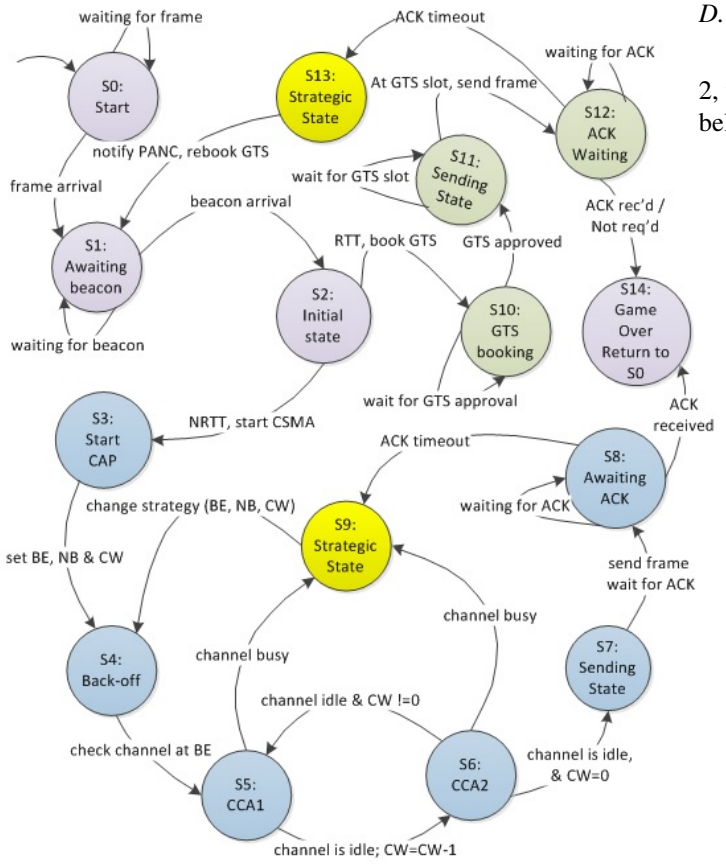

Fig. 2: IoT Game States Transition Diagram

C. Initial States Transition For CAP and CFP

- s_0 - s_2: These states are common to both CAP and CFP. They are preliminary states in which the choice of access method between CAP and CFP is made based on whether the packet is classified as real time traffic (RTT) or non-real time traffic (NRTT).
- s_0: This is the entry point for both CAP and GTS, in which the node wait for the arrival of the packet to be transmitted, the node moves to s_1 after the arrival of a packet (frame).
- s_1: The node wait for the arrival of a beacon to signify the beginning of a super-frame. After the arrival of the beacon, the node move to s_2 to choose between CAP and GTS.
- s_2: At s_2 the node make a choice between CAP (CSMA/CA) and the CFP (GTS) depending on whether the packet is sensitive to delay or not.
- s_3 - s_9: These are the states in CAP with CSMA-CA as the channel access mechanism.
- s_{10} - s_{13}: These are the states in CFP with GTS as the channel access mechanism.
- s_{14}: This state is also common to both CAP and CFP hence it is similar to s_0 - s_2. It signifies successful packet transmission so it marks the end of game session and a transition to s_0, the beginning of another game.

D. The CAP and Its Mechanism

1) CSMA-CA Game States Transition: As shown in the Fig. 2, the transition of state in the CSMA-CA of CAP is discussed below:

- s_2: This is for Non-Real Time Traffic (NRTT) packet, node choose CAP CSMA-CA, initialise its contention parameters and move to s_3.
- s_3 - s_9: These refer to states in CAP with CSMA-CA as the channel access mechanism.
- s_3: At s_3 the nodes initialises it contention parameters: BE, NB and CW, and then move to s_4 to perform a Clear Channel Assessment (CCA) after waiting for Beacon Exponent (BE) period.
- s_4: The node performs a CCA and move to s_5.
- s_5: At s_5, the node decrement CW by 1 and move to s_6 if the channel is idle otherwise it move to s_9.
- s_6: At s_6, the node check its CW and the channel. If the channel is busy it move to s_9. If the channel is idle and the Contention Window (CW) is not equal to zero it return to s_5 to decrement CW otherwise it move to s_7 to send it packet.
- s_7: At s_7, the node send its data and move to s_8 to wait for ACK.
- s_8: At s_8 the node wait for the ACK, if the ACK arrives on time or it's not required, then the node moves to s_{14}, end of the game from which it can return to s_0 the entry point. If the node time out while waiting for the required ACK, then it move to s_9.
- s_9: This state is the strategic state for CAP. It signifies the node suffers unsuccessful transmission or CCA. It is the state in which the contention parameters are manipulated to reverse the trend of unsuccessful transmission or CCA.

2) CSMA-CA Algorithm: The CSMA-CA algorithm is controlled with three variables: NB, BE and CW. The number of Backup (NB) is the number of times a device back-off while attempting the current transmission, In order words, it is the number of trials a device made before the transmission become successful or the threshold number is reached and the CSMA/CA terminates in failure and the packet is discarded. It resets to zero for every new packet. The Beacon Exponent (BE) is associated with number of back-off slots a device will wait before attempting to access the channel. The MAC sub-layer waits for a random number of back-off periods in the range 0 to $2^{BE} - 1$. After the waiting time, the MAC requests the physical layer to performs a CCA. So this random waiting time is controlled by the value of the parameter BE.

The Contention Window (CW) refers to the contention window length and it initialized to 2 in the default IEEE 802.15.4 whenever the channel is assessed to be busy, i.e. It signifies the number of back-off periods the channel must be clear of activity before the device can start transmitting. In other words, after observing the channel to be idle, a node decrement its CW and wait for a back-off period and then perform the CCA again to check if the channel is still idle and then decrement its CW to zero before making a transmission

attempt, thus for a default IEEE 802.15.4, a node will perform CCA twice in order to reduce its CW from 2 to zero before sending its frame. For a CSMA-CA, the strategy of any playing nodes is to manipulate these three parameters in order to win the channel during CCA and transmit their frame, however the CW is of interest to us in this study.

After performing CCA in s_4, the node move to s_5. At state s_5 if the channel is idle it decrements its CW and proceed to state s_6 otherwise it move to state s_9. At state s_6, it repeat a CCA and move back to state s_5. At s_6 if the channel is still idle it decrement the CW by 1 to 0, and move to state s_7 in readiness to send its frame, otherwise it goes to state s_9. It send the packet at state s_7 and move to state s_8 to wait for ACK if required. If ACK frame is received at state s_8, the cycle is completed and the node move to state s_{14}, the end of the game from which it can return to state s_0 the initial state, for another game round. However, if the required ACK is not received in sate s_8, the node transits its state s_9. The state s_9 is the CAP strategic state we introduced. The original algorithm does n't have this, and each time a node transits to this state, it signifies that there is a communication problem that needs to be addressed.

The original algorithm will return to back-off state s_4 whenever the channel is found busy in state s_5 or s_6 but we introduce the state s_9 as a strategic state in which a node evaluates the state of the game and change its strategy base on its knowledge of the game which refers to the number of its transmission failure(s), and its own energy level. In other words, instead of simply retuning to state s_4 to back-off as we have it in the original model, we decided to introduce a strategic state s_9 where the node can do some optimisation and select the best strategy of play based on state of the game and its energy level and then return to s_4 to contest for the channel with optimised parameters that will increase its chance of successful CCA and data transmission.

Energy Level	Contention Window (w)	Probability P_i	Utility U_i
High	0	1.00	$T/1E_a$
Medium High	1	0.50	$T/2E_a$
Normal	2	0.33	$T/3E_a$
Low	3	0.25	$T/4E_a$
Critical	4	0.20	$T/5E_a$

TABLE I: Energy Level and Contention Windows

3) Energy-aware CSMA-CA: The relationship between the contention w_i, available energy E_a, channel access probability (i.e. probability of sending a packet regardless of whether it will be a successful transmission or not) p_i and Utility U_i in our CAP strategic state s_9, is as shown in Table I. In our strategic state s_9, we set the CW size as follows: zero for nodes that has very high energy level, 1 for nodes that have moderately high energy level, 2 for nodes with medium size energy level (default mode), 3 for nodes with low energy level, and 4 for nodes with energy in critical level as can be seen in the Table I. In other words, CW is dynamic and will be inversely proportional to the level of energy available E_a to the node at the time of contesting for the channel.

This implies that high energy nodes can afford to set their CW to zero or very low value, in order to transmit as soon as possible and hence they can achieve more throughput at the risk of packet loss and energy wastage. This is analogous to a city trader who has plenty of cash to gamble with, at the prospect of gaining more but also at the risk of losing some of the cash. On the other hand, nodes with very low energy level will optimise its strategy by setting their CW high to prevent packet loss due to collision, while trying to achieve the desired throughput using their available energy. This is analogous to a city trader who has little cash to gamble with, hence he will carefully choose his gambling trade to reduce the risk of losing part of the little cash while trying to get the best out of it. So the decision of what value of CW is to be used in a misbehaviour scenario is based on the evaluation of the energy level of each node and the decision is to be taken in the strategic state s_9 that we introduced.

E. The GTS and Its Mechanism

1) GTS Game States Transition: As shown in the Fig. 2, the transition of state in the GTS of CFP is discussed below:

- s_2: For Real Time Traffic (RTT), the node sends a GTS booking request to PANC and move to s_{10}.
- s_{10} - s_{13}: This refers to states in CFP with GTS as the channel access mechanism.
- s_{10}: In s_{10} the nodes wait for GTS booking approval from PANC and move to s_{11} on arrival of GTS approval.
- s_{11}: In s_{11} the nodes wait for the allocated GTS time slot. It send its packet at the GTS slot and move to state s_{12}.
- s_{12}: At s_{12} the nodes wait for ACK if required. If the node time out while waiting for ACK, it moves to state s_{13} otherwise it moves to state s_{14}, end game.
- s_{13}: This state is the strategic state for CFP. It signifies that the node suffers unsuccessful transmission. It is the state in which the GTS request parameter is manipulated to reverse the trend of unsuccessful transmission.

2) GTS Algorithm: In the GTS mode, there is no need for CCA since the channel is exclusively reserved for the node that booked each slot. Its mechanism is similar to Time Division Multiple Access (TDMA) mechanism. The channel sharing is achieved by dividing the signal into different time slots, one after the other, each node using its requested and reserved time slot as approved and confirmed by the PANC. Therefore, after sending a GTS booking request to the PANC in state s_2, the node will move from state s_2 to state s_{10} and wait for GTS approval. On receiving GTS approval from PANC, the node move from state s_{10} to state s_{11}, the sending state, and wait for the allocated time slot.

At the allocated time slot, the nodes does not need to do a CCA since the channel has been exclusively reserved for it for that period of time. It just sends its data and move to state s_{12} to wait for ACK, if required. If ACK arrives on time, then the nodes move to state s_{14}, to signify the end of a successful game round. It will then return to state s_0 for a new game

session. However, if the node timed out while waiting for ACK in state s_{12}, that will signify a packet loss for some reasons and so the node will move to the GTS strategic state s_{13}. This state is added by us to enables nodes to notify the PANC of transmission failure of a real time (or emergency) packets, so that the PANC can prioritise the request by reallocating the next available GTS slot or create a slot from the inactive period and allocate it to the node.

3) Energy-aware GTS: The GTS mechanism is independent of CW since it is a contention free transmission, packets are send at the allocated GTS slot without any need for CCA. In theory, the channel is assumed to be cleared for the specific node to legitimately transmit its packet in that slot, so technically speaking it should be a collision free transmission. However, in practice, this may not be the case as a result of misbehaviour of other nodes in the network. Therefore, we have to play another strategy in s_{13}, which is our strategic state for GTS. In the event of a GTS packet loss, the 2 options we considered are: either to locate the misbehaving node(s) and allocate punishment to them or prioritise the retransmission of the lost packet as soon as possible. We choose to implement the latter, because we believe that sending a high priority packet (such as fire or burglar alarm packets or packets that relate to a deteriorating heart beat of an hospital patient) to its destination should take higher precedence.

So our solution to this is that the sending node should book another GTS slot, but with increased priority. In order to achieve the desired elevated priority in the GTS slot request, we introduced a priority variable, PV into the GTS request which is initialise to 0 for every new packet. The PV is incremented by 1 for each retransmission for nodes with high or moderate energy level while the PV is incremented by 2 for nodes with low or critical energy level. A threshold value of 8 is set for PV, at which the packet is either transmitted successfully or discarded. Whenever the PANC receive the a GTS slot request of higher PV, it will prioritise such request by creating additional slot in the inactive period if the CFP is fully booked. This way the priority packet can get transmitted in the next available Beacon Interval (BI).

IV. Analysis Of The Dynamic Game Model

We denote the contention window and channel access probability of a node as w, p_i respectively, then using [13] and [5] we express our channel access equation as:

$$p_i = 1/(w+1) \tag{1}$$

The channel access probability is the probability of node accessing the channel by sending it packets which is different from the probability of successful transmission. The lower the contention window w, the higher the channel access probability p_i. This means that for a node to have a higher access probability, it needs to make use of low contention window. The original CSMA algorithm in CAP initialises the value of CW to 2 for every new packet to be transmitted or after a transmission failure. The CW is then decremented by 1 after each successful CCA until it value reduces to zero before the node can transmit its frame.

A. The Energy Used

Suppose we consider voltage V_n and current I_n across a wireless node connected in a series circuit with known resistor R. We know that, the input current I_n across the wireless node and I_r across the resistor R are equal and can be expressed as the ratio of voltage across the resistor v_r to the value of resistor R. Therefore we can estimate the energy used by the wireless node in the time interval $t_1 - t_0$, according to [5] as:

$$E_{t_0 \ldots t_1} = \frac{V_n}{R} \bar{v}_r (t_1 - t_0) \tag{2}$$

Similarly, according to [5], the idle energy consumption of a wireless network interface over an interval of time $t_1 - t_0$ can be expressed as:

$$E_{idle} = \frac{V_n}{R} v_{(idle)} (t_1 - t_0) \tag{3}$$

We can therefore estimate energy used in transmitting as the difference between (2) and (3).

$$E_u = (t_1 - t_0)(\bar{v}_r - v_{idle}) \frac{V_n}{R} \tag{4}$$

We define the variable available energy E_a on the nodes as the difference between the initial energy (i.e total energy) E_t and energy used in transmission E_u.
i.e $E_a = E_t - E_u$ and hence using (4)

$$E_a = E_t - (t_1 - t_0)(\bar{v}_r - v_{idle}) \frac{V_n}{R} \tag{5}$$

B. The Utility

In our assumption in session 3, we have expressed utility U_i as T/E_u. In a wireless network, energy is a limited resource, therefore, for a given level of available energy E_a, the strategy of the node is to make use of E_a to derive the best utility T/E_u from its usage. Therefore we redefine our utility function as the pay-off or revenue derived from channel access which we expressed as theoretical throughput T per available energy E_a, since the available energy E_a will be used, and hence eventually become energy used E_u in order to get the desired throughput. We use the concept of mixed strategy by denoting the probability of channel access of node i as p_i, then the utility function of a player, U_i can be redefined as a measured of throughput it wants to achieve per the available energy, assuming all nodes are forward looking, as a result of which they want to get the best throughput from the available energy.
i.e :

$$U_i = \frac{p_i T}{E_a} \tag{6}$$

By substituting (1) in (6), we have:

$$U_i = \frac{T}{E_a} \frac{1}{(w+1)} \tag{7}$$

We now optimise U_i by solving (7) with respect to CW w. If we examine (7) closely, we will discovered that the maximum

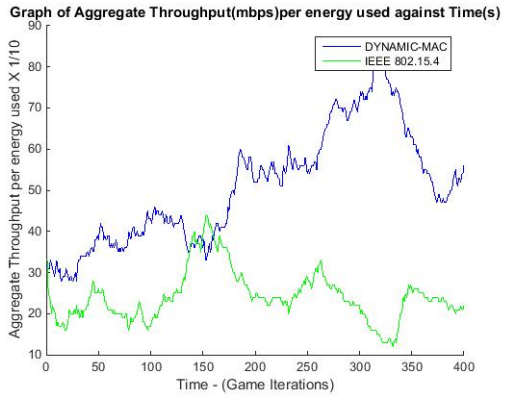

Fig. 3: Throughput/energy for 400 rounds of game cycle.

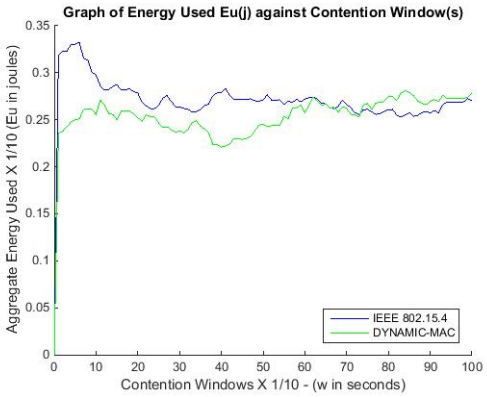

Fig. 5: Energy Used against Contention Window.

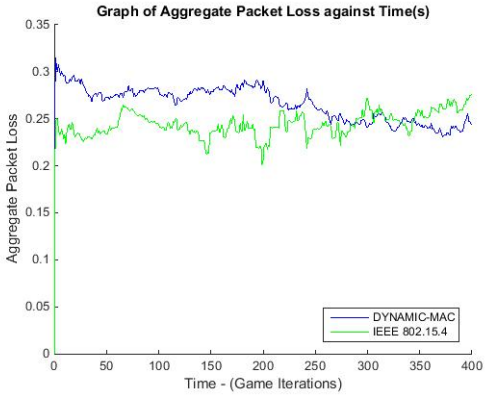

Fig. 4: Packet loss for 400 rounds of game cycle.

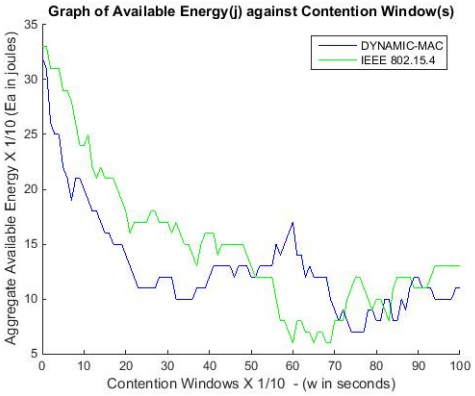

Fig. 6: Available Energy against Contention Window.

value for U_i will occur at $w = 0$ if we keep E_a constant for all the nodes since we assigned the initial energy to the nodes. This implies that setting the $w = 0$ should give the highest value for U_i regardless of the strategies that the other $n - 1$ nodes might be playing. Similarly, the best response strategy for the $n - 1$ nodes, in theory, will be to set their $w = 0$, thus playing Tit-For-Tat (TFT) strategy. However, the available energy for each of the nodes varies based on their loads, energy used in previous transmission or wasted in retransmission. Therefore, according to our algorithm, the $n - 1$, will not to set their $w = 0$, but will rather set it to a value $w = x$, where $x > 0$ and is inversely proportional to their available energy. This is to save energy while trying to maximize their utilities. This is what we coined as adaptive strategies in our game since each nodes will constantly and independently work out the value of w that is best for it, base on its E_a, which correspond to the dynamic equilibrium for the game. As far as we know, this is a new concept which we believe will save energy in IoT.

C. The CSMA-CA and GTS Strategy

In our modelling, we describe the strategy of each nodes as the process of maximizing its utility by choosing contention parameter (for CAP) in strategic state s_9 or GTS slot request parameter (for CFP) in strategic state s_{13} base on its available energy E_a, regardless of the strategies that the other nodes might be playing. This involves optimization of the utility equation (7) for CAP and selecting the appropriate PV in GTS. The dynamism of our game is the fact that nodes can modify their strategies base on the state of the game and their available energy. In other words, by the state of the game, we mean number of failed transmission attempts which will motivate the nodes to change its strategy based on it available energy E_a.

The available energy E_a is the refers to the energy left from all previous transmission. In real life scenario, energy is loaded into the nodes from factory. It may be rechargeable or non-chargeable depending on the design and the usage of the device. In all cases, however, available energy E_a is always the difference between initial energy loaded from factory and the energy used so far. i.e. $E_a = E_t - E_u$. For our simulation run, we allocate initial energy E_t to the nodes, and subsequently recalculate the available energy E_a by deducting the energy used E_u, in transmission and retransmission from the initial energy allocated E_t.

D. Simulation Result

We compare the performance of our dynamic game model by using MATLAB-based Probabilistic Wireless Network Simulator (Prowler) [14]. We simulated a non-cooperative

wireless environment in which there are 8 rational nodes, with the same amount of packets load and energy assigned to all nodes. However 4 nodes were made to played the IEEE 802.15.4 in it default mode while the remaining 4 played our dynamic game with ability to change their strategy subject to their available energy by modifying their contention / GTS request parameters. The simulation was run for 400 game iterations and the combined utilities T/E_u, throughput per energy used during simulation were graphed for the 2 classes of nodes. The resulting graph is as shown in shown in Fig: 3, while the corresponding packet loss graph is as shown in Fig: 4.

The result shows a significant improvement on the throughput per energy used for dynamic MAC over the default implementation of IEEE 802.15.4. However the dynamic MAC tend to loss more packet than the default implementation of IEEE 802.15.4. This is particularly observable at the beginning of the game when all nodes are loaded with the same amount of energy. This was as a result of modifying their contention parameters based on their high energy value in order to achieve better utility. Their throughput and packet loss reduces as the level of their energy reduces, hence they become adaptive to their situations.

Similarly, the graphs of energy used E_u and available energy E_a against contention window size is as shown in Fig. 5 and Fig. 6. An interesting observation on the graphs in the Fig. 5 and Fig. 6 is the fact that, as the energy level of a node playing dynamic MAC game begins to dwindle, it starts to increment its contention window so as to save energy. At the conclusion of the game, the dynamic MAC player actually saves more energy than the default implementation that keeps its contention window parameter constant at the default value 2. This is shown on the energy used graph in Fig. 5 and available energy graph in Fig. 6, which is why we describe our model as energy-aware model and named it as a dynamic game with adaptive strategy.

V. Conclusion

We demonstrated that the IEEE 802.15.4 MAC protocol could be made adaptive to misbehaviour by modelling the protocol as a game, with nodes as the players, with the capability to modify their contention parameters in order to improve their utility in a misbehaviour scenario. The dynamic MAC model defaults to the standard IEEE 802.15.4 under normal condition. That is to say, it operates like a the IEEE 802.15.4 under normal condition, the adaptive strategy kicks in only when the state of the game changes as may be indicative by loss of utility, and nodes returns to the default IEEE 802.15.4 after the transmission of its current packet.

The limitation of our model lies in the assumption that all nodes have the same level of load: fully saturated. This has its advantages and disadvantages. On one hand this means the model is based on fully saturated nodes which is a worst case scenario that may not be reached in most cases, while on the hand it does not accounts for the reality of variation in loads level. We leave the investigate of this as a future work.

We therefore conclude that, although the mechanisms of CSMA-CA and GTS are well known, making them resilient to misbehaviour in the context of IoT is a new concept to the best of our knowledge, and is worthy of further investigation and development. Similarly, a dynamic algorithm that modifies the contention parameters of a node subject to the available energy on the node, in order to achieve a better utility is also a new concept, as far as we know. We hope these ideas will be developed further and ported to other areas of communication and resources sharing, as the concept of IoT continues to evolve, thus moving the world to a smarter world.

References

[1] R. Caceres and A. Friday, "Ubicomp systems at 20: Progress, opportunities, and challenges," *Pervasive Computing, IEEE*, vol. 11, no. 1, pp. 14–21, January 2012.

[2] S. Sajjad and M. Yousaf, "Security analysis of ieee 802.15.4 mac in the context of internet of things (iot)," in *Information Assurance and Cyber Security (CIACS), 2014 Conference on*, June 2014, pp. 9–14.

[3] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 3, pp. 1389–1406, Third 2013.

[4] H. Li, B. Xue, and W. Song, "Application and analysis of ieee 802.14.5 security services," in *Networking and Digital Society (ICNDS), 2010 2nd International Conference on*, vol. 2, May 2010, pp. 139–142.

[5] J. Abegunde, H. Xiao, and J. Spring, "Resilient tit-for-tat (rtft) a game solution for wireless misbehaviour," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug 2015, pp. 904–909.

[6] R. Daidone, "Experimental evaluations of security impact on ieee 802.15.4 networks," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*, June 2011, pp. 1–2.

[7] L. Mokdad, A. Abdelli, and J. Ben-Othman, "Detection of greedy behavior in wsn using ieee 802.15 protocol," in *Modelling, Analysis Simulation of Computer and Telecommunication Systems (MASCOTS), 2014 IEEE 22nd International Symposium on*, Sept 2014, pp. 106–111.

[8] C. Chen, Q. Pei, and X. Li, "A gts allocation scheme to improve multiple-access performance in vehicular sensor networks," *Vehicular Technology, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[9] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Energy cost of security in an energy-harvested ieee 802.15.4 wireless sensor network," in *Embedded Computing (MECO), 2014 3rd Mediterranean Conference on*, June 2014, pp. 198–201.

[10] S. Boyer, J.-M. Robert, H. Otrok, and C. Rousseau, "An adaptive tit–for–tat strategy for ieee 802.11 csma/ca protocol," *International Journal of Security and Networks*, vol. 7, no. 2, pp. 95–106, 2012.

[11] B. Cao, G. Feng, and Y. Li, "A game-theoretic approach for cooperative transmission strategy in wireless networks," in *Global Communications Conference (GLOBECOM), 2012 IEEE*. IEEE, 2012, pp. 1698–1703.

[12] G. Piro, G. Boggia, and L. Grieco, "A standard compliant security framework for ieee 802.15.4 networks," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, March 2014, pp. 27–30.

[13] M. Yan, L. Xiao, L. Du, and L. Huang, "On selfish behavior in wireless sensor networks: A game theoretic case study," in *Measuring Technology and Mechatronics Automation (ICMTMA), 2011 Third International Conference on*, vol. 2, Jan 2011, pp. 752–756.

[14] S. H. Chagas, J. B. Martins, and L. L. de Oliveira, "An approach to localization scheme of wireless sensor networks based on artificial neural networks and genetic algorithms," in *New Circuits and Systems Conference (NEWCAS), 2012 IEEE 10th International*, June 2012, pp. 137–140.