A Stochastic Game for Adaptive Security in Constrained Wireless Body Area Networks

AmelArfaoui*‡, Ali Kribeche‡, Asma ben Letaifa†, Sidi Mohammed Senouci‡, Mohamed Hamdi*
*Digital Security Unit, SupCom University of Carthage, Tunisia
‡DRIVE EA1859, Univ. Bourgogne Franche Comté, France
†MEDIATRON Lab., Sup'Com, University of Carthage, Tunis, Tunisia
{amel.arfaoui, Sidi-Mohammed.Senouci, Ali.Kribeche01}@u-bourgogne.fr, {mmh, asma.benletaifa}@supcom.rnu.tn

Abstract— **Using Internet of Things (IoT) in the health domain is one of the most promising approaches which offer a ubiquitous healthcare where sensors are used, in real time, for constant monitoring of patient's symptoms and needs wherever he is. Wireless body area network (WBAN) is a highly suitable communication tool for the medical IoT devices. However, the conception of WBAN applications is still a challenging job that should take into consideration many technical requirements such as network lifetime, security level, network throughput and data criticality and prioritization. As a consequence, a trade-off between security effectiveness, energy efficiency, and QoS requirements can be perceived as a major performance objective. In this paper, we propose a stochastic game to balance the tradeoff between network performance and security level while taking into account the context dynamics. Simulation results show that the proposed approach can achieve an acceptable security level and is more efficient than benchmark algorithms in terms of network lifetime and throughput.**

Keywords- IoT, Health, WBAN, Game theory, Nash Equilibrium Adaptive security, QoS requirements.

I. INTRODUCTION

The rapid technological advancements of wireless communication and sensing technologies have paved the way for the emergence of the Internet of Things (IoT). It is a megatrend in next-generation technologies that offers tremendous potential solutions for a wide range of applications and particularly e-healthcare which represents one of the most attractive application areas for the IoT [1]. Wireless body area network (WBAN) is a highly suitable communication tool for the medical IoT devices. However, the open nature of wireless communication makes the patient's sensitive data prone to being eavesdropped, modified, injected, or replayed [2]. Therefore, security and privacy are growing concerns in WBAN that need a special attention while taking into account the body sensors' limited resources and context changes.

In WBANs, both security and system performance are primary requirements. Nevertheless, harsh environmental conditions and severe resource constraints of body sensors in terms of communication and computational capacity and buffer size make security costs become more tangible through energy depletion and performance degradation. Moreover, typical channel characteristics in WBANs such as high interference level and human body fading effects increase the risk of data drop and data error. Aside from that, failures in timely delivery of patient's data can impact severely his condition. Therefore, traffic prioritization with QoS guarantee is primordial.

In such stochastic (random) environment, an effective way to handle problems cited above will be to provide an adaptive security based on the appropriate network and system information (the available resources in the specific context). Therefore, we propose a stochastic game for adaptive security to ensure a trade-off between security effectiveness, energy efficiency and QoS requirements. The context dynamics where smart things operate can be modeled using Markov decision process (MDP) to optimize the network's desired objectives. Particularly, a body sensor node, as a decision maker, adopts an adequate policy and then transits from a state to another. The MDP model allows a balanced design to fit the environment conditions and dynamically optimize the network performance because the static decision may lead to inefficient resource utilization.

The main contributions of this paper are threefold. First, we identify the dynamic context changes. Specifically, we consider the heterogeneous and dynamic traffic load, the channel characteristics and threat model. Second, we study the tradeoff between adaptive security effectiveness and network performance via a stochastic game formulation. Finally, we prove the model efficacy and efficiency in terms of security level, energy consumption, and throughput.

The remainder of this paper covers the following points: the proposed context-awareness modeling is described in Section III. In Section IV, we present the stochastic game formulation for adaptive security under uncertain environment. Section V describes the performance evaluations. Conclusion is drawn in section VI.

II. RELATED WORK

Recently, combining security and quality of service (QoS) in the design and management of the IoT has attracted particular attention from researchers. Many studies were mainly based on game theory for performance optimization and it has been widely applied to avoid conflicts and make decisions [3].By making an assessment of all possible situations, players will receive payoff according to their choices which can evaluate the efficacy of adopted strategy and then help the system to reach the optimization. In [4], authors proposed a Stackelberg game where defender plays the role of leader and the attacker acts as a follower in order to protect sensor nodes from external attacks

based on energy defense budget against the corresponding energy attack budget. In [5], a bargaining game was presented through the cooperating nodes which results in the system Pareto optimality (Nash Bargaining solution) in order to optimize the network reliability in multi-hop Wireless Body Sensor Networks (WBSNs). The utility function determines the allocated bandwidths of cooperated nodes while taking into account dynamic environment, QoS, and fairness of resource allocation. In [6], authors proposed a decision support approach based on game theory in order to minimize security risks caused by sharing user's data with IoT prosumer. A zero-sum game has been formulated between users who select a set of prosumers that optimize their payoffs and an adversary who menaces their private data. In [7], an evolutionary game has been applied to analyze the dynamics of the trust decision in Wireless Sensor Networks (WSNs). The authors studied the evolution of trust strategy where players select the cooperative strategy based on the payoff model expressed by node's trust degree. In [8], the authors proposed a repeated game-theoretic approach to detect and prevent the selfish decision of nodes which go to sleep without permission. The utility function concentrates on the power consumption where the node with higher transmission cost has more chance to enter on sleeping state.

All the aforementioned works focus only on the security at the expense of other aspects such as energy efficiency and reliability and vice versa. For this purpose, it seems essential to guarantee a trade-off between different requirements based on adaptive security. In [9], authors presented a scenario-based approach to recognize and evaluate typical security trade-off situations in the IoT. Based on Event Driven Adaptive Security (EDAS) which aims to monitor and analyze thing-generated security events, their model provided a utility-based assessment method to ensure an optimum tradeoff between various contextual requirements (memory, energy and security) involved in a decision. In [10], authors analyzed security metrics effects from the self-adaptive security perspective. The model closed the adaptive control loop of management of security risks, dynamically taking into account the requirements derived from the security metrics quality criteria to ensure efficiency over time applying the MAPE (monitor-analyze-Plan and Execute) reference model. A game-based adaptive security model for IoT-eHealth application has been proposed in [11]. The authors used the Markov game theory to assess the battery life, the memory capacity, the channel bandwidth and the intruder model in order to determine whether or not messages' authentication should be enabled. They emphasize only a limited set of dynamic context parameters in the IoT-eHealth and don't consider user preferences in terms of traffic prioritization and QoS satisfaction.

III. CONTEXT-AWARENESS MODELING

Different QoS requirements, flexibility, and security are important goals to be achieved for healthcare and medical applications in WBANs while considering limited resources of sensor body nodes. These requirements may vary over time according to the application scenario and also due to network dynamics. In this context, we define the WBAN challenging environment concerning traffic generation, communication channel, battery lifetime, and threat model to design the context dynamics of smart things.

A. Traffic Generation

Traffic arrival and prioritization based on the QoS requirements and current scenario must be considered to make a decision. Therefore, the following properties are required in designing the context:

1. Traffic prioritization: it is essential to satisfy strict delay requirements through QoS provisioning. For this purpose, the traffic generated by biomedical sensors can be categorized into on-demand, emergency, and normal traffic where the highest priority is assigned to emergency traffic, second highest priority is assigned to on-demand traffic and the lowest priority is assigned to normal traffic [12]. The equation to calculate the priority is presented by:

$$P_i = \frac{T_i}{G_i * S_i} \quad (1)$$

where P_i is the traffic priority, T_i represents the traffic class value, G_i is the data generation rate and S_i size in bytes of the particular packet.

2. Traffic load: its status is categorized as low load, moderate load, high load, and overload. It is given by [13]:

$$L_i = \frac{T_{ADP}}{Q_c} \quad (2)$$

where L_i is the load index, $T_{ADP}$is the total amount of data packets, and Q_c represents the queue capacity.

3. Memory capacity: We assume that the communication within the WBAN is such that the queuing process at a smart thing and it is modeled as a Batch Markov Arrival Process (BMAP), which enables more realistic and more accurate traffic modeling [11]. In emergency situations, data packets are scheduled in the high priority queue with arrival rateλ_H. The arrival rate of low priority traffic isλ_L.

B. Communication Channel

The wireless channel is susceptible to interference, signal attenuation, and human body fading effects. Hence, security policies should take into account these random channel fluctuations and unreliability issues.

1. Link capacity: The link capacity represents the amount of information (in bits/s/Hz) which can be transmitted over a noisy channel [14]. It is defined as:

$$C_{ij} = \log(1 + \frac{|h_{ij}|^2}{N_0}) \quad (3)$$

where $N_0$is the noise density of the link, $h_{ij}$is the narrowband channel between transmitter j and receiver i . Since the WBAN under consideration is a multi-hop network, it is possible to use multiple hops to go from a transmitter to a receiver. The capacity is then given by the minimum data rate across the two hops:

$$C = \frac{1}{2}\min(C_{SA}, C_{AD}) \quad (4)$$

where $C_{SA}$the link capacity from the smart thing to aggregator and C_{AD} the link capacity from the aggregator to the destination.

2. Interference model: Interference is generally related to QoS issue but it has great potential to pose serious security

issues in WBAN. The interference level between smart thing i and the aggregator is given as follows [15]:

$$SINR_i^t = \frac{P_i^{TX} L_P(d_i)}{N + \sum_{k \neq i} \alpha_{ik} P_k^{TX} L_P(d_k)} \quad (5)$$

where P_i^{TX} is the transmission power of the transmitter node i; N is the power of the noise at the aggregator; α_{ik} is the rejection factor between the channels associated with the nodes i and k; P_k^{TX} is the transmission power of the interfering node k.

3. Mobility model: Mobility increases the probability of packet loss in WBAN. In such context, attackers may harm the system by injecting a low level of noise into the channel and causing a considerable packet loss. Consequently, the lost packet should be retransmitted which cause a waste of bandwidth, energy depletion, and long delays. For this purpose, the challenge of mobility is that it might induce channel fading and increased BER (Bit Error Rate) caused by body movements and the interference with other nodes from different WBAN. It is modeled by the path loss which is dependent on the distance, d between transmitter and receiver, body shadowing and environment [16].

$$L_P(d) = \overline{L_p(d)} + \Delta B + \Delta F \quad (6)$$

where $L_p(d)$ is the mean path loss, ΔB is a log normal distribution presenting the body shadowing:

$$\Delta B \sim \mathcal{N}(\mu_L, \sigma_L) \quad (7)$$

ΔF is a Nakagami-m distribution modeling the multi-path fading channel:

$$\Delta F \sim Nakagami - m(m, \Omega) \quad (8)$$

C. Energy Consumption

We consider three main energy consumption operations in modeling the energy consumption of each node: data communication, sensing, and data processing. The battery depletion process is represented as follows [17]:

$$E_i(t) = E_i - \sum_{k=1}^{t} (E_i^C(k) + E_i^S(k) + E_i^D(k)) \quad (9)$$

where E_i is the initial battery energy at time 0 and $E_i(t)$ is the remaining energy at time t for smart thing i. E_i^C is the communication energy, which represents the number of packets forwarded by the smart thing. E_i^S, E_i^D present the energy consumed for sensing and data processing respectively. The probability of recovering the battery capacity in one time slot is equal to $e^{-\alpha(B-E_i(t))-\beta(E_i(t))}$ $E_i(t)$<B and 0 otherwise, where B is the battery capacity, α is the decay of the discharge process, and $\beta\,(E_i(t))$ is a staircase function [11].

D. Threat Model

WBAN is vulnerable to internal and external attacks which may include: hello flood, Sybil attack, and DoS. To represent the intruder model, we define the probability of attack which is dependent on the confusion matrix:

TABLE 1. CONFUSION MATRIX

	Identified as affected	**Identified as unaffected**
Affected nodes	True positive (TP)	False positive (FP)
Unaffected nodes	False negative (FN)	True negative (TN)

We consider a compromised node M, a legitimate node L; A+: alarm generation; A-: no alarm. The probability of attack is represented as [18]:

$$P_{att} = P(A^+/\,\mathrm{L}) + P(A^-/\,\mathrm{M}) \quad (10)$$

where $P(A^+/\,\mathrm{L}) = \frac{\mathrm{FP}}{(\mathrm{TN+FP})}$; $P(A^-/\,\mathrm{M}) = \frac{\mathrm{FN}}{(\mathrm{TP+FN})}$

Based on these factors, we define the context as $\chi = \{\mathcal{T}, \mathcal{Q}, \mathcal{E}, \mathcal{C}, \mathcal{M}, \mathcal{I}, \mathcal{A}\}$, where $\mathcal{T}$ is the traffic state, $\mathcal{Q}$ is the memory state, $\mathcal{E}$ is the current energy state, $\mathcal{C}$ represents the state of the link capacity, $\mathcal{M}$ is the mobility level, and $\mathcal{I}$ is the interference level, $\mathcal{A}$ is the state of the attack process. By construction, this context is dynamic and reveals the interplay between the conflicting objectives that should be considered when designing security strategies.

IV. STOCHASTIC GAME FORMULATION

In this section, we present the game-theoretic formulation to ensure a tradeoff between security, energy consumption and QoS in WBAN. It is represented as <S, A, r^1, r^2, r^3, P >. S is the discrete state space. A is the action space. r^k is the stage payoff function for player k=1,2,3. P: S×A ↦Δ(S) is the transition probability map, where Δ(S) is the set of probability distributions over S.

A. Adaptive security strategies

In order to prevent and reduce the impact of attacks on the weak radio links and heterogeneous traffic, we propose an adaptive security policy based on environment changing through a set of transition probabilities. The important features of the proposed scheme are: i) to provide an acceptable security level, ii) ability to maintain energy efficiency as high as possible and iii) a well-balanced network performance between different requirements.

The main idea of the approach is that a thing acting as a relay should authenticate the source of the traffic it forwards. Obviously, this considerably reduces the probability of attacks like DoS, Hello flood, Sybil attack….. Nonetheless, it also reduces the lifetime of the relay nodes and increases the delay of sensitive traffic transmission. In the following, we present different adaptive strategies to define adaptive security policies based on these simple rules. These strategies adapt individually to the components of the dynamic context defined in the previous section. We suppose that a smart thing state depends on its observation of the current context, it can be in the secure mode or in the passive mode. In the secure mode, it systematically authenticates the forwarded packets while no security check is performed in the passive mode. An adaptive security policy is modeled by the transition probabilities between these two states. Specifically, when the traffic state is tn, the queue state is q, the current energy state is $E_i(t)$, the link capacity state is c, the mobility level is m, the interference level

is *snr*, and the security level is *s*, the transition probabilities are given by:

$P_{\pi\to\sigma}(tn,p,E_i(t), c,m,snr,s)=P(P(t)=passive|P(t\text{-}1)=secure)$
$P_{\sigma\to\pi}(tn,p,E_i(t), c,m,snr,s)= P(P(t)=secure|P(t\text{-}1)=passive)$

In the following, we define different adaptive strategies that should be considered for making a decision based on the context model presented in the previous section.

1. Adapting to traffic Nature: in emergency situations, the smart thing switches to the passive mode because it is primordial to send the high-priority traffic on time and it turns to secure mode if the traffic priority is low.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ \lambda=\lambda_H\ and\ D_H<t_{QoS}\\ 0 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_1 & if\ \lambda=\lambda_n\ and\ D_n<t_{QoS}\\ 1-\varepsilon_1 & otherwise\end{cases} \quad (11)$$

where n∈ {L, M}, λ_i the arrival rate of packets and $D_i$is the end-to-end delay, i ∈ {H,M, L}, t_{QoS} is a predefined delay threshold.

2. Adapting to Memory: given that the energy depletion is highly related to the number of packets *p* transmitted, the node decides whether to enforce packet authentication or not based on the number of packets in the queue. When this number exceeds the queue capacity$\bar{q}$, authentication is deactivated with probability ε_2 because the risk of blocking legitimate packets increases. Whereas, when the queue capacity is greater than a minimum threshold$\underline{q}$, the smart thing switches from passive mode to secure mode with probabilityε_3 .

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_2 & if\ p\geq\bar{q}\\ 1-\varepsilon_2 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_3 & if\ p\leq\underline{q}\\ 1-\varepsilon_3 & otherwise\end{cases} \quad (12)$$

3. Adapting to link capacity: When the channel state is degraded, the link capacity decreases below a given threshold $\underline{c}$and transmission becomes more expensive. Consequently, energy efficiency is prioritized.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ c\leq\underline{c}\\ 0 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}0 & if\ c\leq\underline{c}\\ 0.5 & otherwise\end{cases} \quad (13)$$

4. Adapting to interference: As the interference affects energy consumption and the throughput. The smart thing privileges saving power when SINR is below a threshold $\underline{\gamma}$. On the other hand, SINR is a prevailing security threat in WBAN. Furthermore, the node switches on secure mode if its level exceeds a threshold $\bar{\gamma}$.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_4 & if\ \gamma\leq\underline{\gamma}\\ 1-\varepsilon_4 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_5 & if\ \gamma\geq\bar{\gamma}\\ 1-\varepsilon_5 & otherwise\end{cases} \quad (14)$$

5. Adapting to mobility: considering that patient's mobility and posture can have a significant effect on efficient packet delivery, it seems more efficient that smart thing goes to passive mode if the path loss is greater than $\overline{PL}$ and it switches to secure mode if the path loss is minimal $\underline{PL}$.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ PL\geq\overline{PL}\\ 0 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ PL\leq\underline{PL}\\ 0.5 & otherwise\end{cases} \quad (15)$$

6. Adapting to energy: The smart thing state turns to passive mode if the energy state is below a threshold $\underline{E_0}$ and it switches to the secure mode if the energy state is greater than $\overline{E_0}$.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ E_i(t)/B\leq\underline{E_0}\\ 0 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ E_i(t)/B\geq\overline{E_0}\\ 0 & otherwise\end{cases} \quad (16)$$

7. Adapting to threat model: based on the probability of detection, the smart things can evaluate the probability of attack and make the decision to switch to secure mode according to the security state (undetected compromised state, masked compromised state, active attack state, vulnerable state…). We define a high threshold of detection$\overline{pd}$ and a low threshold $\underline{pd}$ such that.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_6 & if\ pd\geq\overline{pd}\\ 1-\varepsilon_6 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}\varepsilon_7 & if\ pd\leq\underline{pd}\\ 1-\varepsilon_7 & otherwise\end{cases} \quad (17)$$

8. Hybrid adaptation: This strategy relies on combining different criteria to decide whether to prioritize security or privilege network utility. The mixture of these policies is strongly related to application's requirements. For instance, we can define a strategy where security activation is triggered by the link capacity, the traffic nature, and the current energy state.

$$P_{\pi\to\sigma}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}1 & if\ \frac{E_i(t)}{B}\leq\underline{E_0}, c=c_0, \lambda=\lambda_H\ and\ D_H<t_{QoS}\\ 0 & otherwise\end{cases}$$
$$P_{\sigma\to\pi}(tn,p,E_i(t),c,m,snr,s)=\begin{cases}0.5 & if\ \frac{E_i(t)}{B}\geq\overline{E_0}, c\leq\underline{c}, \lambda=\lambda_M\ and\ D_M<t_{QoS}\\ 0 & otherwise\end{cases} \quad (18)$$

B. Payoff functions

Based on the analytical models mentioned in the previous sections, we propose a stochastic game formulation where the decision-making of players is always dominated by environmental conditions to set up the parameters of the adaptive security policy. The multidimensional utility function indicates the conditional authentication of the forwarded traffic

and its impact on security policy violation, packet blocking, and packet dropping. We consider a damage function, denoted by Δ, which returns the efficiency of the security policy in mitigating the intrusion, and network utility functions, which represent the impact of the security mechanisms on the lifetime of the network and the QoS requirements in terms of throughput. We adopt the sigmoid function to express the utility functions because different QoS requirements are well characterized in the sigmoid form, where it is known that there are different parameters involved, thus leading to the adjustable utilities according to the different requirements[19]. The utility functions are defined as follows:

$$\begin{aligned}\Delta(P_{pv}) &= (1+e^{-g_{pv}.(P_{pv}-h_{pv})})^{-1}\\ \Lambda(P_{pdrop}) &= 1-(1+e^{-g_{pdrop}.(P_{pdrop}-h_{pdrop})})^{-1}\\ \Phi(P_{pb}) &= 1-(1+e^{-g_{pb}.(P_{pb}-h_{pb})})^{-1}\end{aligned} \quad (19)$$

where P_{pv}, P_{pdrop}, and P_{pb} are the probabilities of security policy violation, packet dropping, and packet blocking, respectively, g_{pv}, g_{pdrop} and g_{pb} determine the sensitivity of the utility functions, and h_{pv}, h_{pdrop}, and h_{pb}represent the inflection points.

A security policy violation occurs when false alarms are generated or the security queue is full and then the incoming packets checks are disabled. Packet dropping is related to energy depletion when the smart thing switches to the sleep mode for recharging and bad channel state which increases transmission delay. Packet blocking occurs when the traffic load is heavy and the number of packets in the queue exceeds its capacity. The utility function presented above express a trade-off between prioritizing the security policy (at the risk of depleting the battery, increasing delays and decreasing throughput) and forwarding unchecked packets (at the risk of violating the security policy). Based on this trade-off, we formulate a multilateral Nash Bargaining model where Nash equilibrium can be determined so that utilities are maximized. The players of the game are the adaptive security policy, the energy decay process, and the QoS requirement in terms of throughput presented by the number of successfully received packets during the network lifetime *T*. They execute random strategies to reach equilibrium and release a trade-off between security-effectiveness, energy-efficiency and QoS satisfaction. In this game, the decision-making is based on transition probabilities defined by the vector ε = (ε1, ε2, ε3, ε4, ε5, ε6, ε7). Adjusting different probabilities grants an efficient controlling of the policy violation, packet dropping and packet blocking, thereby impacting the damage, lifetime and throughput functions. In addition, the disagreement outcome in our case is found at the point (0, 0, 0).This point represents the damage, lifetime and throughput values when no agreement can be achieved between the players.

C. Nash equilibrium

Solving the following multi-objective optimization problem defines the Nash equilibrium which is denoted by ($\Delta^*, \Lambda^*, \Phi^*$):

$$\max_{\varepsilon}\left(1-\Delta(P_{pv})\right).\Lambda(P_{pdrop}).\Phi(P_{pb}) \quad (20)$$

The existence of the Nash equilibrium for the proposed game is easily deduced given that justified by the fact that the optimization problem mentioned above is defined on a compact. The equilibrium solution requires the computation of the probabilities P_{pv}, P_{pdrop}, and P_{pb}. For this purpose, we define the state transition matrix for the security policy. Firstly, we define the transition processes related to the energy state, the channel, and memory.

$$E^{(p)} = \begin{pmatrix} E_{0,0}^{(p)} & E_{0,1}^{(p)} & & & \\ E_{1,0}^{(p)} & E_{1,1}^{(p)} & E_{1,2}^{(p)} & & \\ \ddots & \ddots & \ddots & & \\ & E_{b,b-1}^{(p)} & E_{b,b}^{(p)} & E_{b,b+1}^{(p)} & \\ & \ddots & \ddots & \ddots & \\ & & & E_{B,B-1}^{(p)} & E_{B,B}^{(p)} \end{pmatrix} \quad (21)$$

where $E^{(p)}$ is a (B + 1) × (B + 1) matrix representing the transition probabilities between energy states *b* and *b'* when the *p* packets are in the memory and *B* is the battery capacity.

$$C^{(snr,m)} = \begin{pmatrix} C_{0,0}^{(snr,m)} & C_{0,1}^{(snr,m)} & & & \\ C_{1,0}^{(snr,m)} & C_{1,1}^{(snr,m)} & C_{1,2}^{(snr,m)} & & \\ \ddots & \ddots & \ddots & & \\ & C_{k,k-1}^{(snr,m)} & C_{k,k}^{(snr,m)} & C_{k,k+1}^{(snr,m)} & \\ & \ddots & \ddots & \ddots & \\ & & & C_{K,K-1}^{(snr,m)} & C_{K,K}^{(snr,m)} \end{pmatrix} \quad (22)$$

where $C^{(snr,m)}$ is a (K + 1) × (K + 1) matrix representing the transition probabilities between link capacity states *k* and *k'* for a given *snr* and mobility levels.

$$Q^{(tn,p)} = \begin{pmatrix} q_{0,0}^{(tn)} & \cdots & q_{0,P}^{(tn)} & & & \\ \vdots & \vdots & \ddots & \ddots & & \\ q_{R,0}^{(tn)} & \cdots & q_{R,R}^{(tn)} & \cdots & q_{R,R+P}^{(tn)} & \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ & q_{p,p-R}^{(tn)} & \cdots & q_{p,p}^{(tn)} & \cdots & q_{p,p+R}^{(tn)} \\ & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix} \quad (23)$$

Matrices $Q^{(tn,p)}$ represent the changes in the number of packets with different priorities in the queue from *p* to *p'*. *R* indicates the maximum number of packets that can be transmitted; *P* is the maximum number of packets that can arrive.

We denote by A = $(a_{k.l})$ the transition probabilities matrix between the previous state where *k* packets have been authenticated and the current state where *l* packets have been authenticated. Therefore, the probabilitiesP_{pv}, P_{pdrop}, and P_{pb} are given by:

$$\begin{aligned} P_{pv} &= \frac{\sum_{k=1}^{I}\sum_{l=X-p+1}^{P}\pi_l\left(\sum_{i=1}^{X} a_{\left\lfloor\frac{k}{X}\right\rfloor,\left\lfloor\frac{k}{X}+l\right\rfloor}\right)}{E(A)}\\ P_{pdrop} &= \sum_{E_i,c,p,k}\pi(\mathrm{tn},\mathrm{p},E_i(t),\mathrm{c},\mathrm{m},\mathrm{snr},\mathrm{k})\\ P_{pb} &= \frac{\sum_{p,k}\sum_{j=X-p+1}^{P}\left(\sum_k Q_{p,p+l}^{(tn,p)}\right).(j-(X-p)).\pi(\mathrm{tn},\mathrm{p},E_i(t),\mathrm{c},\mathrm{m},\mathrm{snr},\mathrm{k})}{\sum\lambda_n}\end{aligned} \quad (24)$$

where *X* is the size of the queue; *p* is the number of packets in the current state; *P* is the maximum number of packets that can be transmitted in the current state; $\left(\sum_{i=1}^{X} a_{\left\lfloor\frac{k}{X}\right\rfloor,\left\lfloor\frac{k}{X}+l\right\rfloor}\right)$ indicates the total probability that the number of authenticated packets in the queue increases by *l*; π is the steady state probability matrix, obtained through the resolution of the equations π. A = π and π.1 = 1, where 1 is a matrix of ones.

To reduce the complexity of the computation of the Nash equilibrium (20), we adopt the Pareto efficiency which is defined by the state where it is impossible to make any player better off without making at least one individual worse off.

V. PERFORMANCE EVALUATION

In this section, we evaluate the adaptive security policies under the dynamic context through simulation using Matlab. Our main purpose is to find the optimal policy that maximizes the objective function.

A. Simulation environment and Setup

The simulation environment is based on the IEEE 802.15.4 specifications, where the packet size is 1024 bits. We assume a communication model with different link quality, where a bit error rate (BER) is assigned to indicate excellent (PRR: 0.99) and bad (PRR: 0.5) link quality. The channel model involves the node transmission power (- 10dBm), receiver sensitivity (-84.7dBm), noise floor (-102dBm), an additive white Gaussian noise (AWGN) of mean zero and σ=dBm as well as the path loss exponent (3.6) [20]. The path loss model is defined by a path loss at reference distance PL (d_{ref}) =23.49dB, an average deviation σ_{dB}=2.93 and reference distance d_{ref}=0.5cm [21]. The battery capacity is initiated at 1.35Wh for the Shimmer nodes used to collect patient's data [11]. We consider a set of 20 Shimmer nodes where 20% of the total nodes generate emergency traffic, the on-demand traffic presents 30% of the total nodes and the normal traffic constitutes 50% of the total traffic generated during each time slot. The game-theoretic approach is implemented based on Multilevel-µ-Tesla (MµTesla) authentication scheme and compared with Node Capture Game (NCG) [11].

In this work, we focus on three performance metrics; sensor's lifetime, security level and throughput, which have the direct impact on the WBAN performance.

- *WBAN lifetime* is defined as the residual energies of WBAN nodes at each time slot,
- *Probability of security violation* is defined as the probability of attack detection being below a given threshold,
- *Throughput* is defined as the sum of the number of successful packets forwarded to a particular node in a given period of time.

B. Comparison of different strategies

First, we study how the lifetime, damage and QoS functions are affected when a smart thing adopts different strategies according to dynamic context changes for the case where $\varepsilon_1=\varepsilon_2=\varepsilon_3=\varepsilon_4=\varepsilon_5=\varepsilon_6=\varepsilon_7=0.5$. Then we demonstrate the effectiveness of the proposed adaptive security stochastic game by comparing proposed adaptive security policies to the MµTesla technique and Node Capture Game (NCG) [11].The lifetime, damage and QoS functions are depicted in blue, red and green respectively. Figure 1 compares the different strategies where adapting to mobility, interference level, memory, energy and traffic nature strategies achieve a higher sum of successful packet transmission than adapting to intruder given that the throughput is highly dependent on traffic priority, channel characteristics and residual energy. We can ensure a great satisfaction level for a long period and up to 1000 time slots. For the adapting to intruder strategy, when all packets are authenticated the queue will be full faster and then the blocking probability will increase leading to a limited satisfaction level.

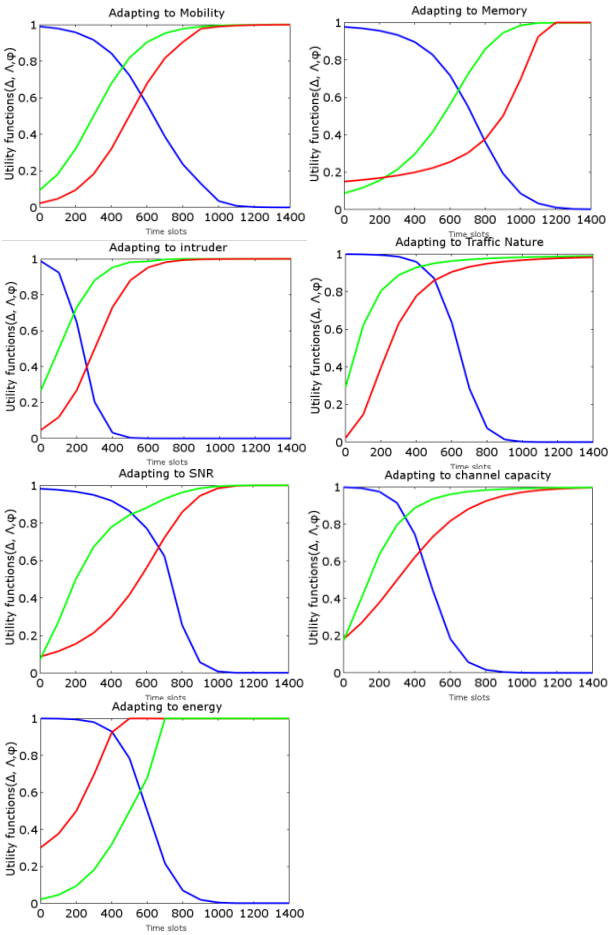

Fig. 1. Performance comparison of different strategies

Now another comparison between MµTesla, NCG and different strategies, the adaptive strategies according to traffic nature, memory and channel characteristics provide around 40% throughput improvement. The results of this comparison are shown in fig. 2. From security and lifetime perspective, we can see that payoff achieved by adapting to energy and intruder strategies are unfair because they consider only one aspect. For adapting to intruder strategy, we can guarantee a high-security level near to this ensured by MµTesla protocol. In such situations, more conservative measures lead to a lower performance where the energy is depleted after around 500 time slots. For adapting to energy strategy, the energy is depleted after 1000 time slots but the security violation rises rapidly. However, making a decision based on the communication channel, traffic nature and memory provide more convenient results for both security and network lifetime which can be extended up to 40% and 48% for adapting to mobility and memory strategies respectively. Therefore, smart things should consider different requirements in order to dynamically

changing their strategies and achieving the desired payoff. The best choice is to adopt the strategy that ensures a well-balanced trade-off between security level, WBAN lifetime and QoS requirements.

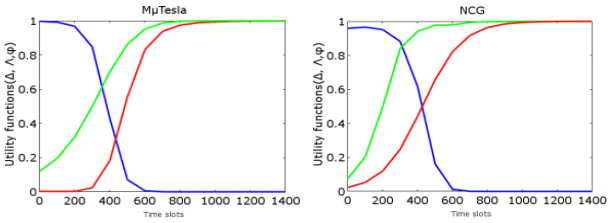

Figure 2: Benchmark techniques

VI. CONCLUSION AND FUTURE WORK

In this paper, we studied the adaptive security methodology while considering distinct context features and sensor nodes capabilities in order to provide a trade-off between security and WBAN performances. We developed a model that is based on a stochastic game between different requirements where a smart thing makes a decision to authenticate forwarded packets or not after environment observation. Then, we evaluate different adaptive strategies and find the optimal policy that should be adopted. We demonstrate the efficiency of our proposed approach as compared to security game and MµTesla authentication protocol where the throughput improvement can reach 40% and the WBAN lifetime is extended to 48%. In the future, we will consider security and privacy threats and implement an intrusion detection system based on the trust level of different actors in WBAN.

REFERENCES

[1] Z.Pang, "Technologies and architectures of the Internet-of-Things (IoT) for health and well-being'' M.S. thesis, Dept. Electron. Comput.Syst, KTH-Roy. Inst. Technol., Stockholm, Sweden, Jan. 2013.

[2] Juha Partala, Niina Keranen, Mariella Sarestoniemi, Matti Hamalainen, Jari Iinatt,Timo Jamsa, Jarmo Reponen and Tapio Seppanen, "Security threats against the transmission chain of a medical health monitoring system", IEEE 15th International Conference on e-Health Networking, Applications and Services, Healthcom,2013.

[3] Mohamed S. Abdalzaher, KarimSeddik, MahaElsabrouty, Osamu Muta, Hiroshi Furukawaand Adel Abdel-Rahman," Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey", Sensors 16(7):1003, June 2016

[4] Mohamed S. Abdalzaher1, Karim Seddik2, Osamu Muta3, and Adel Abdelrahman, "Using Stackelberg Game to Enhance Node Protection in WSNs", 13th IEEE Annual Consumer Communications and Networking Conference, Jan.2016

[5] Pal, R.; Gupta, B.; Cianca, E.; Patel, A.; Kaligotla, S.; Gogar, A.; Wardana, S.; Lam, V.T.; Ganguly, B. "Playing 'games' with human health the role of game theory in optimizing reliability in wireless health networks", In Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), Nov. 2010.

[6] G Rontidis, E Panaousis, A Laszka, T Dagiuklas, P Malacaria, T Alpcan, "A Game-Theoretic Approach for Minimizing Security Risks in the Internet-of-Things", IEEE International Conference on Communication Workshop (ICCW), June 2015

[7] Shen, S.; Huang, L.; Fan, E.; Hu, K.; Liu, J.; Cao, Q., "Trust dynamics in WSNs: An evolutionary game-theoretic approach", J. Sens. 2016, 10.1155

[8] Ben Abid, I.; Boudriga, N., "Game theory for misbehaving detection in wireless sensor networks", In Proceedings of the International Conference on Information Networking (ICOIN), Jan. 2013.

[9] Waqas Aman and Einar Snekkenes, "Managing Security Trade-offs in the Internet of Things Using Adaptive Security", IEEE 10th International Conference for Internet Technology and Secured Transactions, Dec.2015

[10] Antti Evesti , Habtamu Abie, Reijo Savola, "Security Measuring for Self-adaptive Security", Proceedings of the 2014 European Conference on Software Architecture Workshops, Aug.2014

[11] Mohamed Hamdi, Habtamu Abie, "Game-Based Adaptive Security in the Internet of Things for eHealth", IEEE International Conference on Communications, June.2014.

[12] I. Anjum, N. Alam, M. A. Razzaque, M. Mehedi Hassan, and A. Alamri, "Traffic priority and load adaptive MAC protocol for QoS provisioning in body sensor networks," International Journal of Distributed Sensor Networks, 2013.

[13] M. U. Hossain, Dilruba, M. Kalyan, M. R. Rana, and M. O. Rahman, "Multi-dimensional traffic adaptive energy-efficient MAC protocol for wireless body area networks," in Proceedings of the 9th International Forum on Strategic Technology (IFOST '14) ,Oct.2014.

[14] Stéphane van Roy, Franc¸ois Quitin, LingFeng Liu, Claude Oestges, Franc¸ois Horlin, Jean-Michel Dricot and Philippe De Doncker, "Dynamic Channel Modeling for Multi-Sensor Body Area Networks", IEEE Trans. Antennas Propagat.,2013.

[15] Muhammad Mahtab Alam, Elyes Ben Hamid, "Interference Mitigation and Coexistence Strategies in IEEE 802.15.6 based Wearable Body-to-Body Networks", 10th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM), Oct.2015.

[16] Slawomir J. Ambroziak, Kenan Turbic, Carla Oliveira, Luis M. Correia, Ryszard J. Katulski, "Fading Modelling in Dynamic Off-Body Channels", 10th European Conference on Antennas and Propagation, April.2016.

[17] Jae-Joon Lee, Bhaskar Krishnamachari and C.-C. Jay Kuo, "Impact of Energy Depletion and Reliability on Wireless Sensor Network Connectivity", In Proceedings of the SPIE Defense and Security, 2004.

[18] T. Bonaci, L. Bushnell, "Node Capture Games: A Game Theoretic Approach to Modeling and Mitigating Node Capture Attacks," Proc. Second International GameSec Conference, Maryland, USA, 2011.

[19] Chungang Yang, Jiandong Li, Waleed Ejaz, Alagan Anpalagan Mohsen Guizani,"State Utility function design for strategic radio resource management games: An overview, taxonomy, and research challenges", Transactions on Emerging Telecommunications Technologies Journal, May.2016

[20] Mohamad Ali, Hassine Moungla, Ahmed Mehaoua, "Energy Aware Competitiveness Power Control in Relay-Assisted Interference Body Networks", arXiv:1701.08295v1, Jan.2017

[21] Yangzhe Liao, Mark S. Leeson, Matthew D. Higgins and Chenyao Bai,"Analysis of In-to-Out Wireless Body Area Network Systems: Towards QoS-Aware Health Internet of Things Applications", Journal ectronics, 2016.