A Life Time Model for IoT Devices Under Energy Attacks

Yasin Murat Kadioglu

Abstract The Internet of Things (IoT) is a growing and vital computing technology that can monitor the physical environment for both indoor and outdoor applications. In some cases, it is not convenient to connect IoT devices to the power grids. Hence, these devices are often powered by the renewable batteries, which can recharge themselves by harvesting the free energy from the ambient environment. Since devices have to deal with the certain interruptions without enough available energy, attackers might design energy depletion attacks by targeting the device batteries. These attacks cause service interruptions and prevent sustainable operations. Thus, this paper suggests a modelling approach to evaluate the potential impacts of some energy depletion attacks on the battery life-time of IoT devices and networks.

1 Introduction

The Internet of Things (IoT) is an emerging technology which interconnects objects and things by using radio frequency identification and wireless sensor network communication technologies [1]. These devices have an intelligent infrastructure to sense and process information captured from the ambient environment, and to communicate with each other via the Internet [5]. Energy required to operate devices and networks is considered as a crucial issue since the sustainability plays a key role for successful monitorings. In certain situations, it is not possible to provide electrical connections to IoT devices and networks. Therefore, they tend to harvest energy from the environment for extending their battery life-times [3, 4]. In the context of IoT, harvesting energy sources can be divided into two categories [6]: a dedicated

Yasin Murat Kadioglu
Intelligent Systems and Networks Group
Electrical and Electronic Engineering Department
Imperial College, London, SW7 2BT
e-mail: y.kadioglu14@imperial.ac.uk

source (a gateway or a sink node) from which the amount of energy captured by the devices is deterministic, and an ambient source (photovoltaic or wind) in which the amount of energy harvested may vary depending on the environmental changes.

Since maintaining some operations in IoT networks is not possible without a certain level of energy, there has been serious concerns related to the energy depletion attacks causing faster battery depletions. One way of creating such attacks is transmitting useless traffic into the network which elevate the use of energy for each device. In addition, attackers might release electromagnetic emissions to create noise and interference in the networks. This causes the retransmission of the same information. Hence, the retransmissions suppress the effect of elevated the noise and interference at the cost of consuming more energy. It can be seen as a higher transmission power level is required to keep the SINR above (or transmission error probability below) of a certain value.

2 System Model

In this paper, we introduced a model to examine the effects of energy depletion attacks on battery life-time of energy harvesting IoT devices. We assume a network model of K static IoT devices, $\{D_1, D_2, \cdots, D_K\}$, each capable of sensing reliable information from the ambient environment and communicating with a gateway in the network. Figure 1 illustrates the network model. The gateway in the network is assumed to be connected to a power line, and to be capable of transferring certain amount energy to the IoT devices for preventing the interruption of device operations. Therefore, a device battery can be recharged by using either the energy captured from the environment or the energy transferred from the gateway. The energy depletion attacks towards a network force IoT devices create an additional data traffic in the network, and retransmit the same information. We use the following basics in this paper:

1. We assume an IoT device continuously consumes some energy for listening signals (E_l), and harvests some amount of energy both in sleep and awake modes. However, in the awake mode, or in an active duty cycle, the energy consumption is elevated due to data packet sensing (E_s), processing (E_p), receiving (E_r) and transmission (E_t).
2. In each active duty cycle, the device-i consumes constant energy (E_{D_i}) for listening, sensing, processing and receiving subsystems so that it can be defined as:

$$E_{D_i} \triangleq \alpha_{l_i} E_{l_i} + E_{s_i} + E_{p_i} + E_{r_i}, \tag{1}$$

where subscript i stands for the i^{th} IoT device in the network, i.e., D_i. Also, $\alpha_{l_i} E_{l_i}$ represent the fraction of total energy consumption for listening signals in an active duty cycle of D_i.

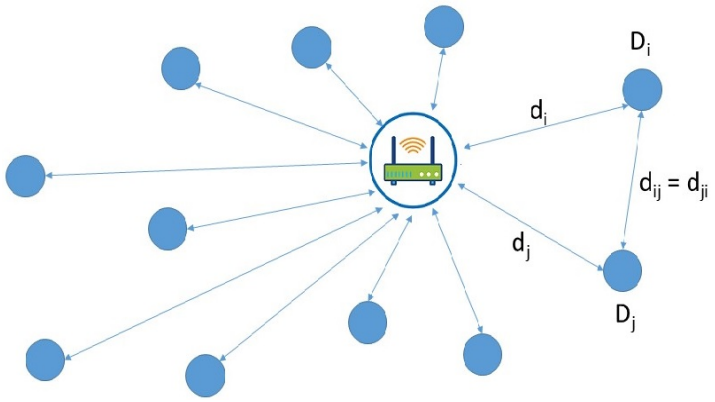

Fig. 1 A network model of K static IoT devices communicating with a gateway.

3. We assume IoT devices in the network also can communicate with each other in the certain situations. Thus, the total energy consumption for the packet transmission per active cycle in D_i can be calculated as:

$$E_{T_i} = E_{t_i} d_i^2 + \sum_{j=1}^{K} \rho_{ij} E_{t_i} d_{ij}^2, \tag{2}$$

where d_i is the distance between the D_i and the gateway. Also, $d_{ij} = d_{ji}$ is the distance between IoT devices D_i and D_j. Another parameter ρ_{ij} represents the packet transmission probability from D_i to D_j in an active duty cycle.

4. The larger distance between two IoT devices may result in the smaller transmission occurrence between them. Therefore, the following product can be assumed as a constant value such that:

$$\rho_{ij} d_{ij}^2 = \frac{\xi_i}{K-1}. \tag{3}$$

Thus, the the total transmission energy consumption per active cycle reduces to:

$$E_{T_i} = E_{t_i}(d_i^2 + \xi_i). \tag{4}$$

5. The total harvested energy in the device D_i is:

$$E_{H_i} = \alpha_{h_i} E_{h_i} + \pi_i \frac{E_g}{d_i^2}, \tag{5}$$

where $\alpha_{h_i} E_{h_i}$ is the harvested amount of energy during an active duty cycle from the ambient environment. In addition, E_g is the determined amount of energy transferred from the gateway to the D_i, which occurs with a probability π_i.

Let the life-time of an IoT device be T in terms of the total number of active duty cycles. Thus, the total energy consumption of the device per active duty cycle, E_{C_i}, directly affects the device life-time, which can be written as the following:

$$E_{C_i}T_i = E_{B_i} + \beta_{h_i}T_iE_{h_i} - \beta_{l_i}T_iE_{l_i}, \tag{6}$$

where $E_{C_i} = E_{D_i} + E_{T_i} - E_{H_i}$ and E_{B_i} is the initial energy level of the D_i's battery. Also, $\beta_{h_i}E_{h_i}$ represents the amount of harvesting energy from the environment by D_i and $\beta_{l_i}E_{l_i}$ represent the amount of energy consumed for listening between two consecutive active duty cycles.. Thus, we can write the following:

$$T_i = \frac{E_{B_i}}{E_{C_i} + \beta_{l_i}E_{l_i} - \beta_{h_i}E_{h_i}} = \frac{E_{B_i}}{E_{C_i} + E_{L_i}}. \tag{7}$$

2.1 Life-time Under Network Attacks

We may also consider the effect of the attacks on the life-time of IoT devices, i.e. how many active duty cycles a device can have before all its energy is depleted. We consider such attacks that will cause an additional data traffic by forcing the devices transmit more data, and will create an extra electromagnetic noise level elevating the transmission errors. In order to suppress the effect of the additional noise level, IoT devices may retransmit the data. Thus, the total transmission energy consumption per active cycle while the devices are under such network attacks can be calculated as:

$$E^A_{T_i} = E_{T_i} + E^a_{T_i} + \eta E^A_{T_i} = \frac{E_{T_i} + E^a_{T_i}}{1-\eta}, \tag{8}$$

where E_{T_i} is the transmission energy consumption without network attacks, $E^a_{T_i}$ is the extra energy consumption due to additional data transmission, and $0 \leq \eta < 1$ is the retransmission probability due to excessive noise increasing with increasing electromagnetic attack level. Note that we assume the same energy consumption for the receiving and processing subsystems. Thus, the battery life-time under the attacks can be calculated as:

$$T^A_i = \frac{E_{B_i}}{E^A_{C_i} + E_{L_i}} \tag{9}$$

where $E^A_{C_i} = E_{D_i} + E^A_{T_i} - E_{H_i}$.

On the other hand, the probability of correctly receiving (or decoding) the packet sent by a given D_i that transmits at power level P_{T_i} be denoted by:

$$e_i = f\left(\frac{\zeta_i P_{T_i}}{N_i + (K-1)\phi_i P_{T_i}}\right) \tag{10}$$

where $0 < \zeta_i < 1$ is the fraction of transmitter power received by the receiver. In addition, f is some decreasing function with its argument, the received power $\zeta_i P_{T_i}$ to noise N_i plus interference $(K-1)\phi_i P_{T_i}$. Since transmitters use different frequency channels, it is assumed $\phi_i < \zeta_i$. However, network attacks aggravate the N_i and ϕ_i values so that the communication errors will increase.

The transmission power P_{T_i} has an interesting effect on the error rates since a) a higher P_{T_i} causes more interference, and b) it also provides the higher power to overcome interference as well as noise and attacks. However, the smaller communication errors require the higher transmission power levels which directly reduces the lifetime of devices. Thus, this interesting trade-off will be illustrated in the next section as well as some numerical examples showing the effect of attacks and the other parameters on the life-time.

3 Numerical Results

Heinzelman et. al proposed an energy consumption model for wireless sensors where the typical amount of energy that a transmitter consumes for the transmission in an active duty cycle is $100nJ/m^2$ [2]. Since the energy consumption is dominated by the communication subsystem, we assume $E_t > E_r > E_p > E_s = E_h > E_l$ whose values can be seen in Table 1.

For the sake of the simplicity, we assume a ring topology network where the gateway is located in the center of the network and the IoT devices are randomly distributed at a distance (or a radius) of d. Figure 2 (left) shows the effect of the radius of the ring topology on an IoT device life-time for different ξ values where we assume other parameters as $\alpha_h = \beta_h = \alpha_l = \beta_l = 1$ and $\pi = 0.1$. The life-time dramatically decreases with increasing radius, since it has a direct effect on E_T and E_H. Also, we can observe the effect of ξ decreases with increasing radius on the life-time, which is due to the fact that E_T becomes dominated by E_t. Figure 2 (right) shows the similar effect for different π values for the same parameter values and $\xi = 0.1d^2$. Although the value of π has a great impact on the life-time for small d values, it's effect almost vanishes for the greater d values since the received transfer energy by the device inversely proportional to the distance square.

Parameter	Description	Value
E_t	Transmission Energy per m^2	$100nJ/m^2$
E_r	Receiving Energy	$80nJ$
E_p	Processing Energy	$50nJ$
E_s	Sensing Energy	$20nJ$
$E_l\alpha_l$	Listening Energy per duty cycle	$10nJ$
$E_h\alpha_h$	Harvesting Energy per duty cycle	$20nJ$
E_g	Energy that gateway can transfer	$200nJ$
E_B	Energy of the battery	$1J$

Table 1 Parameters used for numerical examples

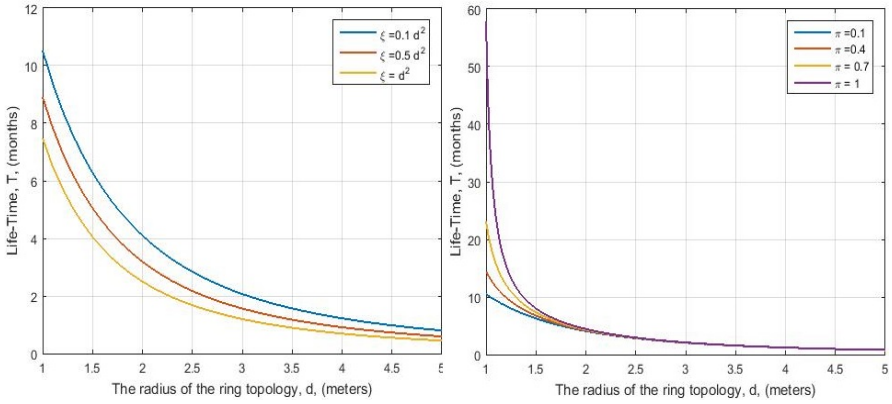

Fig. 2 Life-time of a device according to the radius of the ring topology for different ξ values (left), and π values (right).

Figure 3 (left) shows the effect of the energy consumption E_D in an active duty cycle on an IoT device life-time for different energy harvesting scenarios where we assume $\alpha_h E_h = \beta_h E_h$, $\alpha_l E_l = \beta_l E_l$, $\pi = 0.1$ and $d = 1$. The life-time of a device becomes shorter as a natural result of the more energy consumption. We also observe that as the energy consumption increases, the effect of the energy harvesting on the life-time of a device decreases.

Figure 3 (right) shows the effect of retransmission probability for different values of extra transmissions due to network attacks where the parameter assumptions are same as Figure 3 (left). The increase in both retransmission probability and extra energy consumption due to the additional data traffic cause shorter life-time for a device, as expected.

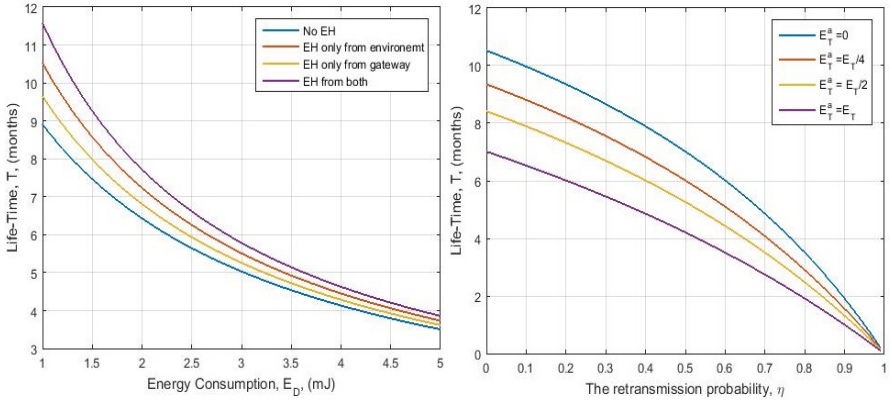

Fig. 3 Life-time of a device according to the energy consumption E_D (left), and the retransmission probability for different E_T^a (right).

Consider a particular device, say the D_i, operating in proximity with a network of K identical devices so that all transmitting at the same power level P_T. Figure 4 (left) shows the effect of increasing noise power due to attacks on the transmission error probability for different interference levels where $P_T = 100nW$, $N = 1$, $\zeta = 0.5$, $K = 10$. We observe that the higher interference results in the higher transmission errors for small noise power levels. However, when the effect of attacks on the noise becomes severe, the effect of interference is almost vanished. On the other hand, Figure 4 (right) shows how the transmission error varies with the increasing transmission power for different interference levels where we assume same parameter values with Figure 4 (left). We observe that the increase in transmission power may overcome the transmission errors for the networks with small interference attacks. However, if the interference level is high, then there will be no significant change of the transmission errors.

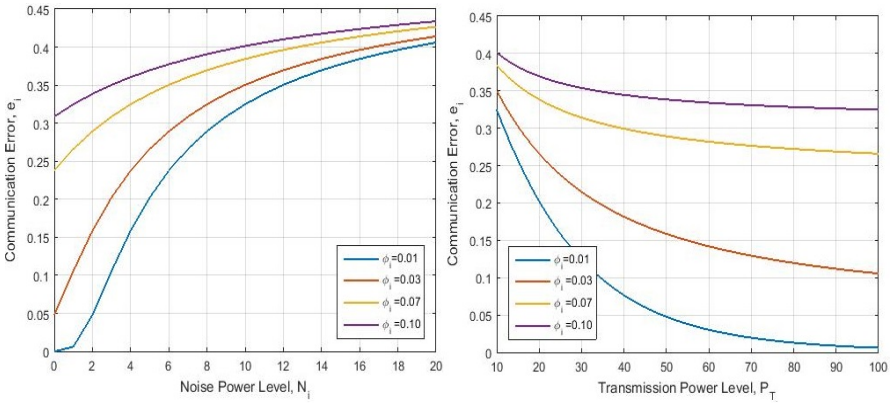

Fig. 4 The effect of the noise power (left), and the effect of the transmission power (right) on the error probability for different interference effects.

4 Conclusion

In this paper, we focused on the life-time of IoT devices that operate in a network where they may suffer from some attacks that attempt to exhaust their available energy. We proposed a model to represent the life-time of an IoT device by considering the number of active duty cycles that the device can accomplish until its battery is completely depleted. We also assume that a device is capable of harvesting energy both in awake and sleep mode, and it continuously consumes energy for "listening" to signals. Attacks can create extra flows of data and traffic information so that the more energy consumption occurs. In addition, noise and interference level can be elevated due to electromagnetic attacks, which causes packet retransmissions as

well as transmission with a higher power level. The analytical models provided to represent such circumstances allow us to obtain numerical results. The results illustrate the effect of the system parameters and energy depletion attacks on the battery life-time of the devices.

Acknowledgements

This research has received funding from the European Unions Horizon 2020 Framework Programme for Research and Innovation through Projects H2020 GHOST under GA No. 740923, and SerIoT under GA 780139.

References

1. S. Abdullah and K. Yang. An energy efficient message scheduling algorithm considering node failure in iot environment. *Wireless Personal Communications*, 79(3):1815–1835, Dec 2014.
2. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on*, pages 10–pp. IEEE, 2000.
3. Y. M. Kadioglu. Energy consumption model for data processing and transmission in energy harvesting wireless sensors. In T. Czachórski, E. Gelenbe, K. Grochla, and R. Lent, editors, *Computer and Information Sciences*, pages 117–125, Cham, 2016. Springer International Publishing.
4. Y. M. Kadioglu. Finite capacity energy packet networks. *Probability in the Engineering and Informational Sciences*, 31(4):477504, 2017.
5. P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan. Wireless energy harvesting for the internet of things. *IEEE Communications Magazine*, 53(6):102–108, June 2015.
6. X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han. Wireless networks with rf energy harvesting: A contemporary survey. *IEEE Communications Surveys Tutorials*, 17(2):757–789, Secondquarter 2015.