Battery Attacks on Sensors

Erol Gelenbe and Yasin Murat Kadioglu

Intelligent Systems and Networks Group
Dept. of Electrical and Electronic Engineering
Imperial College, London SW7 2BT, UK
{e.gelenbe, y.kadioglu14}@imperial.ac.uk

Abstract. In the Internet of Things (IoT), a simple form of attack can try to deplete the energy available to operate the myriads of wireless sensor nodes that will be used. Some of these nodes will use batteries, while others may harvest ambient energy such as photovoltaic, or electromagnetic, or vibration based energy. Thus this paper tries to analyse the effect of such attacks on the energy life-time of such devices. We first briefly survey the types of attacks which aim at the nodes' energy provisioning systems. Then we provide mathematical models that can be used to estimate the effect of attacks that attempt to deplete the energy system for nodes that use energy harvesting.

Keywords: Wireless Networks, Battery Life-Time, Network Attacks, Renewable Energy

1 Introduction

Energy needed to operate networks is known to be an important issue, both for the sustainability of information technology in general, and with regard to the need to operate stand-alone networks in locations where the electrical grid is not available or is not reliable, or when in a given location it is impossible to provide electrical wired connections to all sensors as in pre-constructed buildings which are later equipped with sensors. Thus there has been a growing concern regarding attacks which directly affect the energy consumption of networks [1–3], and which may deplete batteries that are needed to operate certain network nodes.

Such attacks can take three basic forms: they can increase the activity of nodes through useless data packets (DPs) that the nodes receive, and then have to process and respond to, attackers can also use electromagnetic emissions to create noise that will cause high error rates, and hence force them to take corrective action such as packet retransmissions that increase energy consumption and network delays through multiple data retransmissions [4], and attacks can also change the "sleep-awake" duty cycle of nodes and reduce the proportion of time when the nodes should be asleep to save energy. Larger noise levels may also lead to increase in transmission power and hence to shorter battery life time.

2 Prior Work

Prior work has discussed many types of energy depletion attacks. In a simple case known as a *vampire attack*, a vampire node appears to be benign, but it continuously sends protocol compliant messages to other nodes [5] which reply with acknowledgements, and consume energy both in processing the incoming messages from the vampire, and to reply to them. In our analysis, vampire nodes may be causing the traffic of rate λ_A that the node under attack is sending.

Vampire attacks may be adapted to various routing protocols [6]. They have been observed to take one of two forms: the *carrousel* and the *stretch* attack. In the carrousel attack, a vampire node sends corrupted data leading to routing loops. In the stretch attack, artificially longer routes are chosen despite the fact that shorter routes are available. Carrousel attacks result in more energy consumption than stretch attacks [7], and the detection of vampire attacks is not easy since one malicious vampire node can affect the whole network, effectively opposing routing techniques that are usually designed to increase network battery life-time and save energy [8].

Earlier work has introduced packet routing methods for ad-hoc networks that maximise the battery life-time of the network so that it may be used to counter or mitigate vampire attacks [9]. Other power aware routing techniques have been suggested in [10], and a protocol was proposed in [7] to detect and mitigate vampire attacks, providing routing through the network only for legitimate packets, and verifying that consistent progress is made by packets towards the destination. Another study [11] provides a mitigation method for preventing carrousel attacks by adding extra forwarding logic to check whether there are loops in source routes. To prevent stretch attacks, the work in [12, 13] suggests "strict" source routing where the route is exactly specified in the header and there is no need for checking its optimality. An attack packet detection and removal method was proposed in [14, 15], using packet broadcast rates and energy parameters at sensor nodes.

Sleep deprivation attacks are designed to keep sensor nodes awake as long as possible to increase their energy consumption, and reduce the battery life of a sensor from months to days, and also include [1, 16] barrage, synchronization, replay, broadcast, and collision attacks. Typically, a node that receives a request to receive data from another node, can check its routing table to see whether it may receive data from that node; if not. it discards the request and goes to sleep. In sleep deprivation attacks [17], malicious nodes will continuously try to send data to some node(s), so that they cannot sleep and waste energy. As a defense, a lightweight scheme was proposed [18], to activate a node only if it receives messages from authenticated and legitimate nodes. Attackers can also conduct barrage attacks on awake nodes by bombarding them with legitimate requests, causing significant energy wastage. However barrage attacks can be easily detected and require more effort by the attacker, while sleep deprivation attacks require only a single message [19, 17].

Since nodes have a listen-sleep cycle that can be periodically updated to maintain synchronisation among neighbours, attackers may send *artificial syn-*

chronisation packets to lengthen the nodes' awake time [20], causing 30% or more energy depletion due to shorter sleep times, and a possibly 100% increase in data loss due to the misalignment of synchronisations. A defence strategy to mitigate the effects of such attacks was proposed in [20], by ignoring all synchronisation messages with a relative sleep time longer than a pre-set threshold. On the other hand, in a *replay attack* [21], an adversary repeats a valid transmission in the network. Since the attack uses the replay of messages with small changes, it can fool other nodes by convincing them that repeated messages concern a new message exchange. Note that in wireless networks [16] the received signal can help identify malicious nodes through their use of a stronger signal [22].

In *broadcast attacks* [23], malicious nodes broadcast unauthenticated traffic and long messages which must be received by other nodes before being possibly discarded for lack of authentication. Such attacks are hard to detect since they have no effect on system throughput, and nodes that receive them waste energy. In *collision attacks* [24], a hostile node breaks the medium access control protocol and transmits noise packets to corrupt neighbourhood transmissions. Noise packets collide with legitimate packets, and a defence strategy has been proposed [25] based on error correcting codes.

A defence strategy against energy depletion attacks was studied in [16] by considering *denial of sleep attacks* which dramatically increase the energy consumption of a wireless sensor node. Also, different types of denial of sleep attacks such as the barrage attack, synchronization attack and broadcast attack were studied in [19], [20], [23], [26], [18]. An evaluation and attack detection method is proposed in [4] where the quality of service is not necessarily degraded. The method of end-to-end communications reliability based on control packet injections and packets replication is studied in [27]. It is showed that the method is vulnerable to energy depletion attacks and it is impossible to keep safe a protocol from such attacks without authentication. A two-tier secure transmission scheme against energy depletion attacks was proposed in [28] by using the hash-chain to generate dynamic session keys which can provide a mutual authentication key. Also, the detection and the removal of another energy depletion attack, *vampire attack*, based on the routing protocol of the wireless sensor network was studied in [1], [6], [15], [14]. The vampire attacks are very difficult to detect and they basically deplete the resources by continuously repeating the corrupted data or choosing the longer path for the routing data [7]. On the other hand, a hardware based energy attack, *hardware trojans*, studied in [29] where it is showed that a huge energy depletion may occur by embedding a hardware trojan trigger to the integrated circuit.

3 Results Addressed in this Work

In this paper we propose a modeling approach to address attacks that force the node to transmit additional traffic, and which create electromagnetic noise that induces errors and hence packet retransmissions. Two types of nodes are considered, those which use energy harvesting as the only energy supply and

those that use a battery that would have to be replaced at regular intervals, and we develop the following basic aspects:

1. In the energy harvesting node, the node's battery is modeled as an "energy buffer" for energy packets (EPs), whose maximum capacity is E, while he data buffer has a maximum capacity of B DPs. Thus we discretise the representation of the battery, in addition to the usual discretisation of data buffers.
2. A DP waiting in the buffer is allowed to have a time-out after which it is deleted from the buffer, and this time-out is represented by a removal rate γ; obviously when the system does not have time-outs we just take $\gamma = 0$.
3. Similarly, to represent energy leakage, EPs have a leakage or departure rate from the energy buffer represented by the parameter μ.
4. The node sends λ_n DPs per unit time under normal operation (i.e. when it is not being attacked). The traffic of "useless" attack DPs that arrive from the "service network", namely the Internet or a mobile network, to the node and that require a response from the node back into the service network, will result in an additional traffic rate λ_A of DPs being sent out from the node, creating further "useless" energy consumption, and
5. The electromagnetic attack noise that creates DP errors, results in a DP *retransmission* probability $0 \leq r < 1$, so that the noise level reflects in a value of r that increases with the noise level.

As a result, and initial "normal" DP traffic rate λ_n is transformed into a total traffic rate under attack denoted by λ_a that is given by:

$$\lambda_a = \lambda_n + \lambda_A + r.\lambda_a = \frac{\lambda_n + \lambda_A}{1 - r}, \tag{1}$$

because the electromagnetic noise causes errors in all of the traffic, including the traffic of rate λ_A that results from the reply packets that the node sends in response to attack packets. Thus λ_a in (1) represents the total DP traffic that the node sends when it's normal traffic would have been λ_n, thte attack traffic it receives is λ_A and the noise attack causes retransmissions with probability r.

These two types of attacks are considered to compute the energy life-time of a wireless node based on its energy harvesting rate, with nominal or "normal" traffic and the resulting traffic rate in the presence of attacks. The reduction of the node's energy life-time due to attacks is computed and illustrated it with numerical results.

We assume that the node's energy harvesting system has been designed to operate with a nominal value Λ_n of EPs per unit time, which the node is able to harvest in the specific environment that is being considered. The rate Λ_n then results in an acceptable energy life-time T_n when the system is operating normally without attacks, and is sending DPs at rate λ_n.

Similarly, nodes with a fixed battery size of E_0, which we will also measure in units of "energy packets". will have a battery life-time of T_n^b under normal operation when they are supposed to provide for a normal DP traffic rate of λ_n.

Based on these parameters, we can compute the value of the node's energy life-time T_a, for nodes that use energy harvesting, and T_a^b if they use a battery, when they operate under the effect of attacks represented by attack traffic rate λ_A and the effect of electromagnetic noise attacks which create transmission errors and require each DP to be retransmitted with probability r.

Thus, we are interested in finding to what extent the energy life-time of the node has been *reduced* by the attacks, and hence in computing the ratio $\frac{T_a}{T_n}$, or $\frac{T_a^b}{T_n^b}$ as a function of the ratio of attack traffic $\frac{\lambda_A}{\lambda_n}$ and of r.

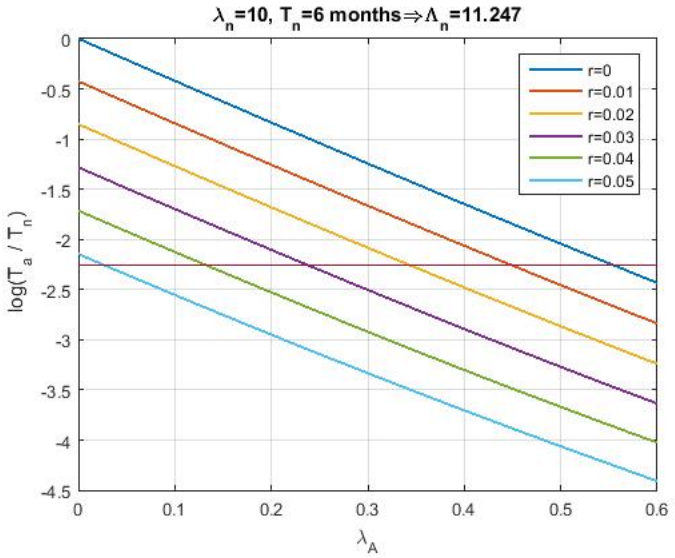

Fig. 1. The curves illustrate the effect of two simultaneous types of attacks, namely the attacks that create added traffic, and those that create retransmissions due to noise that is generated by electromagnetic attacks. We show the variation of the *common logarithm* of the ratio of node energy lifetime under attack, to energy life-time without attacks (y-axis), against the arrival rate of attack traffic λ_A with distinct curves for increasing values of the retransmission probability r due to electromagnetic attacks. The parameter settings are $E = B = 100$, $\gamma = 0.01\lambda_n$ and $\mu = 0.01\Lambda_a$. We fix the "normal life-time" of the system until the battery is emptied after $T_n = 6$ *months* of operation, on average. Thus the EP arrival rate Λ_n representing the required energy harvesting will vary with the normal traffic rate λ_n as shown on each of the graphs. The effect of the attacks is shown by the rapid decrease of the ratio $\log \frac{T_a}{T_n}$ as both λ_A and r increase.

4 A System with Renewable Energy and Finite DP and Energy Buffers

In this section, we use the modeling approach initiated in [30–33] regarding a wireless node that exploits renewable energy sources (such as photovoltaic, mechanical vibrations or electromagnetic scavenging) where the node collects data or energy at a relatively slow pace as compared to the time it takes to transmit a DP over the node's wireless channel which can only take nano-seconds, so that its nominal operating parameters are λ_n and Λ, the latter corresponding to the nominal rate in which it harvests EPs in the environment where it is operating.

While it is under attack, the node transmits λ_a DPs per unit time as indicated in (1), due to both the attack packets it receives, and which require a response from the node producing an additional packet rate λ_A, and also due to the retransmission probability r due to errors caused by electromagnetic noise and interference. Note that the noise may be created by nodes which are attacking the system, while the interference may just be caused by the increased volume of wireless traffic as an indirect effect of attacks that are going on in the network.

The state of the node at time t is represented by the pair N_t, M_t where N_t is the backlog of DPs at the node, while M_t is the number of EPs that it stores at that time. Denoting the node's state probability $p(n,m,t) = Prob[N_t, M_t]$, we know that $p(n,m,t) > 0$ only if $n.m = 0$ because if the node has enough energy, it will immediately attempt to transmit DPs until either all DPs in its buffer have been sent out, or its energy has been depleted.

We assume that the node has a finite capacity of B packets in its data buffer, while its battery can only contain E energy packets. Furthermore, DPs will be removed from the data buffer after a time-out of average value $\frac{1}{\gamma}$ with an exponentially distributed departure rate of γ. Similarly, EP leakage occurs at a rate of μ EPs per unit time.

Defining the stationary state probability distribution $p(n,m) = \lim_{t\to\infty} p(n,m,t)$, we derive the equilibrium equations:

$$
\begin{aligned}
&p(n,0)(\lambda_a + \gamma + \Lambda) = \lambda_a p(n-1,0) + (\Lambda+\mu)p(n+1,0),\ 0 < n < B,\\
&p(B,0)(\Lambda+\gamma) = \lambda_a p(n-1,0),\\
&p(0,0)(\lambda_a+\Lambda) = p(1,0)(\Lambda+\gamma) + p(0,1)(\lambda_a+\mu),\\
&p(0,m)(\lambda_a+\mu+\Lambda) = \Lambda p(0,m-1) + (\lambda_a+\mu)p(0,m+1),\ 0 < m < E,\\
&p(0,E)(\lambda_a+\mu) = \Lambda p(0,E-1),
\end{aligned}
$$

so that

$$p(n,0) = \alpha^n p(0,0),\ 0 < n \le B, \tag{2}$$

$$p(0,m) = \theta^m p(0,0),\ 0 < m \le E, \tag{3}$$

$$p(0,0) = \frac{(1-\alpha)(1-\theta)}{\alpha^{B+1}(\theta-1) + \theta^{E+1}(\alpha-1) + 1 - \alpha\theta}, \tag{4}$$

where

$$\alpha = \frac{\lambda_a}{\Lambda + \gamma},\ \theta = \frac{\Lambda}{\lambda_a + \mu}. \tag{5}$$

Thus the probability that the battery is empty is simply:

$$P_0^a(0) = \sum_{n=0}^{\infty} p(n,0) = \frac{(\alpha^{B+1} - 1)(\theta - 1)}{\alpha^{B+1}(\theta - 1) + \theta^{E+1}(\alpha - 1) + 1 - \alpha\theta}. \tag{6}$$

The expected (average) battery life-time, i.e. the average time it takes the node's battery to empty from the instant at which it contains one EP, can then be obtained from the fact that when the battery empties, on average after $\frac{1}{\Lambda}$ time units it will receive an EP once again, so that:

$$P_0^a = \frac{\frac{1}{\Lambda}}{T_a\ +\ \frac{1}{\Lambda}},\ or\ \ T_a = \frac{1}{\Lambda}[\frac{1}{P_0^a}\ -\ 1]. \tag{7}$$

If we replace λ_a by λ in all terms, then we obtain the average battery life-time when the node is *not* being attacked, namely:

$$T_n = \frac{1}{\Lambda}[\frac{1}{P_0}\ -\ 1]. \tag{8}$$

If the probabilities P_0^a and P_0 are very small, then:

$$\log \frac{T_a}{T_n} \approx \log P_0 - \log P_0^a. \tag{9}$$

Figure 1 shows various curves for the battery lifetime versus the attack traffic rate λ_A and the retransmission error rate due to electromagnetic attacks r, assuming that the normal operating life-time before the system's energy supply is depleted has been set to $T_n = 6\ months$, and $E = B = 100$. In this numerical example, we have set the nominal normal load of the wireless sensor at $\lambda_n = 10\ DPs/hour$ and the energy harvesting rate then needs to be $\Lambda = 11.247\ EPs/hour$ to meet the $T_n = 6\ month$ average energy life-time of the system when it does *not* suffer from attacks.

In Figure 2 we examine the effect of E the energy storage capacity of the system on its energy life-time. So we use all of the same parameters as in Figure 1 fixing $r = 0.06$, and we also take $B = 100$, and set $T_n = 6\ months$ for $E = 100$. But along the x-axis we vary the local storage battery capacity E from 100 to 10^3 and observe the effect on T_a for different values of attack traffic λ_A and observe the resulting effect on T_a.

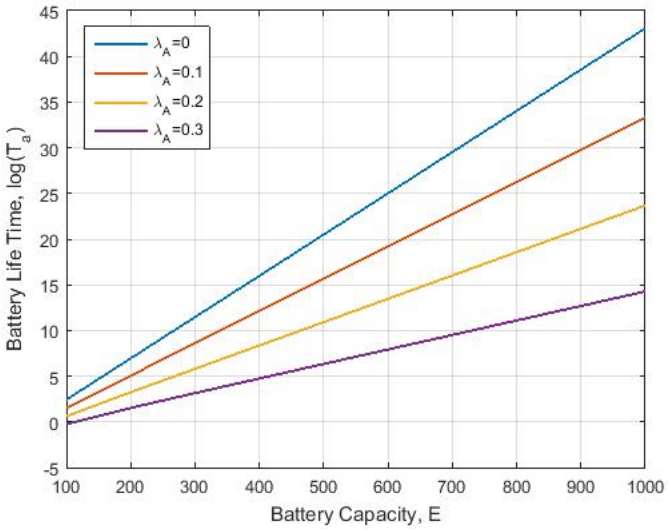

Fig. 2. The node's energy life-time on the y-axis versus the local battery capacity E along the x-axis for different values of attack traffic and $r = 0.06$. As expected, the local battery storage capacity will improve the system performance, but this effect will saturate at large values of E.

5 Conclusions

In this paper we have focused on the effect of simple energy based attacks on sensor network nodes. We consider how long it takes to deplete a battery, and hence stop the node's operations, when a sensor node is being used and the case where the node exploits ambient but intermittent energy sources and therefore does not require being connected to the grid, or being fed by a battery that is replaced from time to time.

Our analysis focuses on the effect of attacks which are meant to deplete the node's energy, either through creating additional "useless" traffic, or which creates electromagnetic noise which genders packet errors and further packet retransmissions. Analytical results and numerical experiments are shown to compare and evaluate the resulting effects.

References

1. A. Dubey, V. Jain, and A. Kumar, "A survey in energy drain attacks and their countermeasures in wireless sensor networks," *Int. J. Eng. Res. Technol*, vol. 3, no. 2, pp. 1206–1210, 2014.
2. F. François, O. H. Abdelrahman, and E. Gelenbe, "Impact of signaling storms on energy consumption and latency of LTE user equipment," in *17th IEEE International Conference on High Performance Computing and Communications, HPCC*

2015, 7th IEEE International Symposium on Cyberspace Safety and Security, CSS 2015, and 12th IEEE International Conference on Embedded Software and Systems, ICESS 2015, New York, NY, USA, August 24-26, 2015, 2015, pp. 1248–1255. [Online]. Available: https://doi.org/10.1109/HPCC-CSS-ICESS.2015.84

3. ——, "Towards assessment of energy consumption and latency of LTE ues during signaling storms," in *Information Sciences and Systems 2015 - 30th International Symposium on Computer and Information Sciences, ISCIS 2015, London, UK, 21-24 September 2015*, 2015, pp. 45–55.
4. V. V. Shakhov, "Protecting wireless sensor networks from energy exhausting attacks," in *International Conference on Computational Science and Its Applications*. Springer, 2013, pp. 184–193.
5. N. Geethanjali and E. Gayathri, "A survey on energy depletion attacks in wireless sensor networks," 2012.
6. S. R. Singh, "Improving the performance of energy attack detection in wireless sensor networks by secure forward mechanism," *International Journal of Scientific and Research Publications*, p. 367.
7. E. Y. Vasserman and N. Hopper, "Vampire attacks: draining life from wireless ad hoc sensor networks," *IEEE transactions on mobile computing*, vol. 12, no. 2, pp. 318–332, 2013.
8. E. Gelenbe and C. Morfopoulou, "A framework for energy aware routing in packet networks," *The Computer Journal*, vol. 54, pp. 850–859, 2011.
9. E. Gelenbe and R. Lent, "Power-aware ad hoc cognitive packet networks," *Ad Hoc Networks*, vol. 2, pp. 205–2016, 2004.
10. E. Gelenbe and T. Mahmoodi, "Energy-aware routing in the cognitive packet network," *Energy*, pp. 7–12, 2011.
11. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless networks*, vol. 11, no. 1-2, pp. 21–38, 2005.
12. A. Kröller, S. P. Fekete, D. Pfisterer, and S. Fischer, "Deterministic boundary recognition and topology extraction for large sensor networks," in *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*. Society for Industrial and Applied Mathematics, 2006, pp. 1000–1009.
13. Y. Wang, J. Gao, and J. S. Mitchell, "Boundary recognition in sensor networks by topological methods," in *Proceedings of the 12th annual international conference on Mobile computing and networking*. ACm, 2006, pp. 122–133.
14. B. Umakanth and J. Damodhar, "Detection of energy draining attack using ewma in wireless ad hoc sensor networks," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 4, no. 8, 2013.
15. M. Soni and B. Pahadiya, "Detection and removal of vampire attack in wireless sensor network," *International Journal of Computer Applications*, vol. 126, no. 7, 2015.
16. D. E. Boubiche and A. Bilami, "A defense strategy against energy exhausting attacks in wireless sensor networks," *Journal Of Emerging Technologies In Web Intelligence*, vol. 5, no. 1.
17. C. P. B. V. Ramanathan, "The resurrecting duckling: Security issues for ad-hoc wireless networks."
18. R. Falk and H.-J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," in *Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on*. IEEE, 2009, pp. 191–196.

19. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *International Journal of Distributed Sensor Networks*, vol. 2, no. 3, pp. 267–287, 2006.
20. X. Lu, M. Spear, K. Levitt, N. S. Matloff, and S. F. Wu, "A synchronization attack and defense in energy-efficient listen-sleep slotted mac protocols," in *Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on.* IEEE, 2008, pp. 403–411.
21. A. Di Mauro, X. Fafoutis, S. Mödersheim, and N. Dragoni, "Detecting and preventing beacon replay attacks in receiver-initiated mac protocols for energy efficient wsns," in *Nordic Conference on Secure IT Systems.* Springer, 2013, pp. 1–16.
22. V. Sharma and M. Hussain, "Mitigating replay attack in wireless sensor network through assortment of packets," in *Proceedings of the First International Conference on Computational Intelligence and Informatics.* Springer, 2017, pp. 221–230.
23. M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC.* IEEE, 2005, pp. 356–364.
24. Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," *ACM Trans. Sen. Netw.*, vol. 5, no. 1, pp. 6:1–6:38, Feb. 2009. [Online]. Available: http://doi.acm.org/10.1145/1464420.1464426
25. H. Chaudhari and L. Kadam, "Wireless sensor networks: security, attacks and challenges," *International Journal of Networking*, vol. 1, no. 1, pp. 4–16, 2011.
26. D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *IEEE transactions on vehicular technology*, vol. 58, no. 1, pp. 367–380, 2009.
27. L. Buttyan and L. Csik, "Security analysis of reliable transport layer protocols for wireless sensor networks," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on.* IEEE, 2010, pp. 419–424.
28. C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sensors journal*, vol. 15, no. 6, pp. 3590–3602, 2015.
29. S. Wei, J. H. Ahnn, and M. Potkonjak, "Energy attacks and defense techniques for wireless systems," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks.* ACM, 2013, pp. 185–194.
30. E. Gelenbe, "Synchronising energy harvesting and data packets in a wireless sensor," *Energies*, vol. 8, pp. 356–369, 2015.
31. E. Gelenbe and A. Marin, "Interconnected wireless sensors with energy harvesting," in *International Conference on Analytical and Stochastic Modeling Techniques and Applications.* Springer, 2015, pp. 87–99.
32. Y.M. Kadioglu, "Energy Consumption Model for Data Processing and Transmission in Energy Harvesting Wireless Sensors" in *International Symposium on Computer and Information Sciences.* Springer, 2016, pp. 117–125.
33. Y.M. Kadioglu, "Finite Capacity Energy Packet Networks" in *Probability in the Engineering and Informational Sciences.* Cambridge University Press, 2017, pp. 1–28.