SECURITY CHALLENGES FOR ENERGY-HARVESTING WIRELESS SENSOR NETWORKS

Alessio Di Mauro[1], Davide Papini[1] and Nicola Dragoni[1]
[1]*DTU Informatics, Technical University of Denmark, Denmark*
{*adma, dpap, ndra*}*@imm.dtu.dk*

Keywords: SECURITY, ENERGY-HARVESTING, WIRELESS SENSOR NETWORK

Abstract: With the recent introduction of Energy-Harvesting nodes, security is gaining more and more importance in sensor networks. By exploiting the ability of scavenging energy from the surrounding environment, the lifespan of a node has drastically increased. This is one of the reason why security needs a new take in this topic. Traditional solutions may not work in this new field. Brand new challenges and threats may arise and new solutions have to be designed. In this paper we present a taxonomy of attacks, focusing on how they change in the energy harvesting scenario compared to regular sensor networks. Finally, we present and discuss existing security solutions for EH-WSNs.

1 INTRODUCTION

A recent trend in the sensor networks field is to equip nodes with energy scavenging units. *Energy Harvesting Wireless Sensor Networks (EH-WSNs)* are regular wireless sensor networks, where nodes have the special capability of recovering some of the energy surrounding them. This energy is then used to power a node. Harvestable sources can vary according to their provenience, their predictability and whether they are controllable or not. Typical sources of scavenged energy are light sources, thermal gradients, radio waves, wind sources, shocks and vibrations. As described in (Sudevalayam and Kulkarni, 2011) the possible architectures are Harvest-Use where the harvested energy is instantly used to energize the node, or Harvest-Store-Use where the energy obtained from the environment is accumulated in one or more storage units such as super-capacitors. In the second case the excess energy is not wasted (unless also the storing unit is full) and the harvested energy source does not have to be constantly present for the node to run. On the other hand additional components have an impact on the final cost of the nodes.

The introduction of energy harvesting radically changes the way to design WSNs. The energy available in a node battery is not bound to monotonically decrease, but it can also increase or maintain its level over time, depending on the availability of the scavenged source. This means that a sensor node can "die" and "come back to life" multiple times. Furthermore, different operations require different amount of energy, with the transmission through the on-board radio generally being the most expensive one (Wander et al., 2005). This requires the node having to choose how to spend its energy, depending on what parameter is considered most important and should therefore be prioritized (e.g. throughput vs availability).

In this paper we provide a taxonomy of attacks for energy harvesting WSNs, we see how scavenging capabilities affect them and if new and specific attacks can be depicted. Moreover, we present a discussion of the current state of the art for security contributions specific to EH-WSNs. Lastly we present some considerations and ideas about such solutions.

The remainder of this paper is organized as follow. In Section 2 we present a classification of security threats for EH-WSNs focusing on the differences with regular WSNs. Section 3 contains an overview of related work for the topic and Section 4 presents some comments and thoughts on it. Section 5 concludes the paper.

2 SECURITY CHALLENGES

Security in WSNs is a well known topic and has been studied for many years. Lots of different attacks have been discovered, implemented and addressed (Lupu, 2009), (Sen, 2010), (Martins and Guyennet, 2010). Specific protocols have been designed to secure dif-

ferent aspects. Despite that, introduction of energy harvesting capabilities is a game changer, a fresh approach is required in order to address the specific challenges that this technology introduces. Imagine a simple scenario where an attacker takes control of one or more than one node. In a regular WSN environment a node would eventually run out of available energy, and the attacker should then take actions in order to keep the attack going, for example by physically replacing the battery of the depleted node or re-deploying the attack on a new target, with all the connected problems and risks. On the other hand in energy harvesting enabled networks, the same identical attack would have a much greater effect due to the extended lifespan of a node. At the same time, an energy depletion attack would completely disrupt a node in a battery powered WSN whereas it should constantly be repeated in an EH-WSN scenario.

The introduction of energy scavenging capabilities completely redefines the typical life cycle of a WSN and so specifically designed approaches are required. While is obvious that the attacks possible on EH-WSNs are a superset of those possible for regular WSNs, it is not clear if and how they behave differently, or if new specific attacks can be deployed.

Taxonomy of Attacks. We provide a classification of attacks in WSNs by defining and exploring three dimensions which the attacker can exploit to perform an attack. These are: (i) Intervention, (ii) Presence and (iii) Time. *Time* dimension relates to the time span the attacker has or needs to perform the attack, it can go from few seconds (e.g. jamming), to several minutes (e.g. hijacking, MITM) to a longer time (if we take into consideration key recovery through mere brute force or direct retrieval from stolen nodes). *Presence* relates to the space domain the attack extends on, it can be local, distributed or global as defined in (Benenson et al., 2008). Finally *Intervention* takes into consideration the actions that the attacker can do. This is the most interesting dimension since it can directly give an idea of possible attacks. We identified eight forms of intervention:
Destruction: the attacker can destroy one or multiple nodes.
Eavesdropping: the attacker can intercept and store messages sent between nodes.
Data Knowledge: the attacker can acquire the data stored on one or multiple sensors (e.g. by dumping the whole memory of a sensor).
Disturb/Partial Data Modification: the attacker can partially modify data on a sensor (e.g. change security parameters).
Full Data Modification: the attacker can fully modify data stored on a sensor (e.g. by direct access to the node or simply by feeding it with data).
Reprogramming: the attacker can reprogram a sensor.
Energy Reduction/Control: the attacker can force the reduction of a node's energy, or control its depletion rate.
Energy Exploit: the attacker can exploit the energy level of a node in a malicious way.

By looking at the list it is clear that in the energy harvesting scenario the last two elements bring to slightly different attack patterns with respect to ordinary WSNs. For space limitation, a complete analysis of the combinations between the three dimension is not within the scope of this paper. The reader can refer to (Lupu, 2009) and (Martins and Guyennet, 2010) for short surveys on attacks on WSNs.

Energy Harvesting. In order to better understand attacks and relate them to energy harvesting, we identified what we call *atomic actions*. These can be composed to build an attack. Most of the atomic actions are not restricted to EH-WSNs only, but can be related to any security threat in every system. We identified three main subset of atomic actions:
Medium/Channel: listen, inject, intercept, destroy, modify, localize, selective block of destination/source commlinks.
Physical: tamper, switch on/off, reduce energy.
Cryptography: break encryption (e.g. key attacks) exploit specific crypto mechanisms (weak random number generator or rekeying methods, wrong implementation, side-channel attacks).

WSNs devices are typically resource constrained in terms of energy and computation. Considering that performing cryptographic operations has an heavy impact in terms of computations and resources needed, and that additional work is required to handle the data overhead (e.g. signatures, keys, padding), it is clear why security has always been a challenge. With EH-WSN energy potentially is not an issue anymore, and computation could also be improved (more energy translates into less need for reduced power computation). This brings a whole new perspective in view and new possible scenarios for security, such as adaptable security levels, waiting queue for highly confidential data (the device transmits data when it has the energy to encrypt it according to its content), more reliable network topology due to the fact that nodes last more time, possibility of multiple duplicated and separated routes.

Obviously this impacts also on the attacker perspective, making it more difficult to break stronger encryption but also giving him other ways of attacking the system. Looking at the *Intervention* dimen-

sion it is clear that the element that changes most with respect to ordinary WSNs is *Energy Exploit*. The atomic actions which are directly connected to this are physical (on/off switching and reduce energy) and cryptography related. By hampering the amount of energy that a device harvests from the environment, an attacker can force the device to lower its security level or to delay the transmission of high sensitive data . Moreover, in an EH-WSN is very likely for a node to go off for long periods and then back on, thus hiding possible attacks that tamper with the device.

EH-WSNs also rely on energy level prediction to perform activities at the best. An attacker could intervene and alter the expected energy level thus forcing the network to behave in an unpredicted or incorrect way. Multiple combinations are indeed possible: an attacker could weaken the energy of a node which is supposed to decrypt a high security level message, thus preventing it to do so. It is very much like a DoS attack, but softer: the node is not completely disabled yet it cannot perform its duties to the expected level.

3 RELATED WORK

Only two interesting results can be found in literature. In both cases an adaptive security mechanism is presented, even though the actual approach used is somehow complementary.

Strength Oriented Approach. The first energy harvesting specific approach for security that we are going to describe is the one presented in (Taddeo et al., 2010). Here the authors consider a sensor network where the traffic is sent from the nodes to the sink. Moreover, they assume the existence of different types of package, where every type has a different priority level and security requirements.

The starting points are the amount of energy available at a given time on a node (considering also the energy harvester contribution), and the amount of energy required in order to send a single packet, specified as the sum of discrete items (such as the energy needed for sending the payload and the energy overhead introduced by cryptography).

The main idea is to provide a list of possible priority levels and supported security suites with different characteristics. The higher the priority level of a packet, the more likely it will be delivered to its final destination. Different security suites instead provide different combinations of security properties (e.g. authentication, confidentiality) with increasing strength (i.e. longer key), at the cost of an higher overhead for the transmission, which translates into an higher amount of energy required to convey the package. By introducing an optimization process, a node is able to choose an adequate security suite depending on the amount of energy available, and to delay packets according to their priority levels.

Time Oriented Approach. The second solution worth mentioning is (Pelissier et al., 2011). It takes a completely different approach: the authors question the adaptability of using block ciphers and propose a scheme that applies to stream ciphers. They point out that in a stream cipher the keystream is independent of the input message, therefore it can be computed separately in advance. So the authors suggest to precompute and store keystream bytes in a buffer, and use them when the energy within the system is scarce.

Under the circumstances of the case study proposed, the authors claim a 14% increase of messages sent from a node that uses a key buffering mechanism compared to one that does not.

As an addition the approach introduces the possibility of having authentication capabilities. To do so the authors implement a Wegman-Carter MAC scheme (Carter and Wegman, 1977) based on the Poly32 universal hash function family (Won, 2001).

4 DISCUSSION

The first proposed approach directly takes advantage of the inherent properties of EH-WSNs. It implements a security system that, based on the available energy and on external constraints, can adapt two opposing factors such as security performance and the node's lifespan. Within these setting the proposed model successfully applies the strongest available security suite and guarantee an high delivery rate for high priority packages.

Here the network topology used could be a major problem for real world applications. Very commonly multihop networks are used in order to cover bigger areas without having to use multiple or mobile sinks. In the discussed approach, by using a star shaped network, two facts always hold true: firstly, the receiver of a packet (i.e. the sink) always has enough energy to unpack the message, and secondly it never has to forward the message to another node. By switching to a multihop network these facts are not true anymore. First of all routing protocols are needed to deliver messages from one end to the other. This could cause a node to form a choke point either because it is the routing choice of reference for a large number of other nodes and so it has to process a lot of messages, or also because its scavenging capabilities are

hindered by physical world circumstances (e.g. a solar panel equipped node is deployed close to a tree and doesn't receive too much sunlight). It is not clear what would happen in one of these scenarios, but it is probably a problem worth further investigating.

Moreover, a system like the one presented could greatly take advantage of harvesting prediction models like (Lu et al., 2010), so that the best choice is not computed locally as the one that instantly maximizes the cipher's strength or the length of the outgoing queue in a greedy manner, but a more proactive approach could be used to provide better performance over a longer period of time. For example by knowing that soon a very good situation for the energy harvester will manifest (e.g. sun is rising, lots of sunlight will be available for a long period) then the current security suite could be kept unchanged even if that wouldn't be the optimal choice in the short run.

The idea proposed in the second work aims at precomputing data when the harvested energy is abundant, and using it when the available amount is reduced to prolong the life of a node. Anyway, the authors of the paper do not discuss matters like the topology of the network and the shape and directionality of the traffic. As discussed before, if the traffic generated by one node is intended to another node rather than the sink, it could be possible that the recipient does not have enough energy to process it (i.e. decrypt it, analyze its content and react). Again, in a multihop network nodes are burdened with the additional task of forwarding packages. This could greatly reduce the time available for a node to compute future keystreams. Furthermore, for node to node communication the keystreams have to be aligned for decryption to happen, and for the verification of MACs keys have to be shared in advance and agreed upon.

An interesting idea could be to rely on other nodes to perform computationally demanding operations when the energy is scarce. A way to do so could be by piggybacking data, such as the keystream bytes for future messages, on regular messages.

5 CONCLUSION

Applications for EH-WSNs are constantly increasing, and so are their security requirements. How to improve these aspects is an interesting open question. In this paper we have provided a taxonomy of attacks for EH-WSNs, we have discussed how scavenging capabilities affect them and if new and specific attacks can be depicted. Afterwards, we have described recent approaches that present two complementary take on the same topic. On one hand we have an adaptation of the strength of the algorithms used according to the available energy, in this way communications can be carried on, at the cost of less secure messages. On the other hand there is a time oriented approach that takes advantage of the decoupling between plain text and keystreams in specific scenarios, so that the latter can be computed in advance when the energy is abundant, and used when it is scarce. Both ideas explain how to exploit characteristics specific of power harvesting systems where the amount of available energy will fluctuate over time both up and down.

Clearly being able to define solutions that can dynamically adapt some of their parameters according to the current available energy, allowing the system to run within acceptable limits in any circumstance is a very critical feature of future EH-WSNs.

REFERENCES

Benenson, Z., Cholewinski, P., and Freiling, F. (2008). Vulnerabilities and attacks in wireless sensor networks. *Wireless Sensors Networks Security*, pages 22–43.

Carter, J. L. and Wegman, M. N. (1977). Universal Classes of Hash Functions (Extended Abstract). In *Proc. of STOC'07*, pages 106–112. ACM.

Lu, J., Liu, S., Wu, Q., and Qiu, Q. (2010). Accurate modeling and prediction of energy availability in energy harvesting real-time embedded systems. In *Proc. of IGCC'10*, pages 469–476.

Lupu, T.-G. (2009). Main types of attacks in wireless sensor networks. In *Proc. of the 9th WSEAS SSIP '09/MIV'09*, pages 180–185. WSEAS.

Martins, D. and Guyennet, H. (2010). Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. In *Proc. of NBiS'10*, pages 313–320.

Pelissier, S., Prabhakar, T., Jamadagni, H., VenkateshaPrasad, R., and Niemegeers, I. (2011). Providing Security in Energy Harvesting Sensor Networks. In *Proc. of CCNC'11 IEEE*, pages 452–456.

Sen, J. (2010). A survey on wireless sensor network security. *CoRR*, abs/1011.1529.

Sudevalayam, S. and Kulkarni, P. (2011). Energy harvesting sensor nodes: Survey and implications. *Communications Surveys Tutorials, IEEE*, 13(3):443–461.

Taddeo, A. V., Mura, M., and Ferrante, A. (2010). QoS and Security in Energy-Harvesting Wireless Sensor Networks. In *Proc. of SECRYPT'10*, pages 1–10.

Wander, A., Gura, N., Eberle, H., Gupta, V., and Shantz, S. (2005). Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. In *Proc. of PerCom'05*, pages 324–328.

Won, D., editor (2001). *Information Security and Cryptology - ICISC 2000, Third International Conference, Seoul, Korea, December 8-9, 2000, Proc.*, volume 2015 of *Lecture Notes in Computer Science*. Springer.