Introducing the Cyber-Physical Attacker to Energy-Harvesting Wireless Sensor Networks

Alessio Di Mauro, Davide Papini, Roberto Vigo, Nicola Dragoni
DTU Informatics
Technical University of Denmark
Kgs. Lyngby, Denmark
{adma, dpap, rvig, ndra}@imm.dtu.dk

ABSTRACT: *Cyber-Physical Systems based on Wireless Sensor Networks are pervading our everyday life,ranging from industrial to military applications. Due to the criticality of the tasks performed by these systems, and to the increasing number of fields in which they are employed, their security is a central concern. What is more, with the recent introduction of Energy-Harvesting nodes, securing such a system is even harder. An EH-node is able of scavenging energy from the surrounding environment, thus extending its lifespan, but this new feature introduces a new target for attackers. Traditional approaches to WSN security may not work in this new domain: new solutions have to be designed to cope with brand new challenges. A taxonomy of attacks is presented in this paper, which focuses on highlighting the novelties of the energy-harvesting context compared to regular sensor networks. We also discuss existing solutions specific to the energy harvesting world, and comment on the trend that this topic is likely to follow in the future. Finally, we sketch a comparison between the cyber-physical attacker we define and adversary models belonging to security protocols verification literature.*

Keywords: Security, Energy-Harvesting, Wireless Sensor Networks

Received: 15 June 2012, Revised 28 July 2012, Accepted 2 August 2012

1. Introduction

Wireless Sensor Networks (WSNs) are collections of nodes able to sense some physical quantity such as humidity, pressure, seismic activity, temperature, air pollution, etc. In its simplest form, a typical node, consists of four main components: the sensor circuitry, a computing unit (usually a micro-controller), a radio transceiver and a power source, making it a self-sufficient entity. Typical applications of sensor nodes include monitoring the area they are deployed across, enabling the overall system to react whenever an alerting condition is recorded. Depending on the dimension of the area to monitor, a WSN can scale up to thousands of nodes, which have then to be inexpensive devices. Moreover, being deployed in wide areas, nodes are usually powered by batteries, and thus they have a pretty short lifespan. These two factors make the alternative of deploying new nodes preferable to collecting and replacing the ones that failed due to hardware malfunctions or exhausted batteries.

A recent trend in the sensor networks field is to equip nodes with energy scavenging units. An energy scavenging unit is a component able to recover some of the energy normally present in the physical environment surrounding a node, and store it in a specifically designed reservoir (e.g. a rechargeable battery or a gold capacitor) so that it can be used at a later time in order to power the node.

This new approach has a deep impact on WSNs design and exploitation. The energy available in a node battery is no more

bound to monotonically decrease, but it can also increase or maintain its level over time, depending on the availability of the scavenged source. Hence, a node that disappears from the network when runs out of power, may later be available again. Moreover, energy-harvesting allows to design control software that highly relies on the amount of available energy in order to take decisions: different operations require different amount of energy, with the transmission through the on-board radio generally being the most expensive one [18]. Depending on the available energy and possibly on scavenging predictions, a node can choose to prioritize a given parameter (e.g. throughput vs. availability).

Finally, the energy-harvesting capabilities have an impact on the system security. The usual view on WSN nodes is that an unreachable node has to be consider untrustworthy, as during an offline period it could undergo a physical attack. Nonetheless, this approach is no longer viable when considering EH-node, since nodes may disappear and come back multiple times. Moreover, new energy-related attacks arise, for instance energy depletion aimed at causing weaker cryptography due to few available energy.

1.1 Contribution of the Paper

The main contribution of the paper is the following. We propose a first threat model for Energy-Harvesting Wireless Sensor Networks. In particular, we provide a taxonomy of attacks in EH-WSNs, we discuss how scavenging capabilities might affect these networks and if new and specific attacks can be depicted.

Moreover, we briefly explore the relationship between our threat model and the capabilities an adversary is generally assumed to exhibit in security protocol analysis. The benefit of the conceptual map we sketch is twofold. On one hand, it opens up for the exploitation of formal methods, successfully used for security protocols analysis, in the verification of WSNs security properties. On the other hand, it highlights that state-of-the-art protocol verification frameworks cannot deal with cyber-physical attackers, sketching thus a line for future work in both directions.

Finally, we do a critical analysis of the current state of the art on security in EH-WSNs, presenting some original considerations and ideas about current solutions.

1.2 Outline of the Paper

The remainder of this paper is organized as follow. In Section 2 we briefly introduce the new concept of energy harvesting WSNs. In Section 3 we present our threat model, including a classification of security attacks for EHWSNs, focusing on the differences with regular WSNs. In Section 4 we look at our threat model from a security protocols verification standpoint. Section 5 contains a critical analysis of related work. Finally, in Section 6 we conclude the paper summarizing its main contribution and highlighting possible future trends in EH-WSNs security.

2. Energy HarvestingWireless Sensor Networks

During the past few years, green technologies experienced a remarkable growth. Environment friendly applications have considerably increased. Furthermore, due to their nature, sensor nodes are usually meant to be as small and as inexpensive as possible so that they can be highly versatile. Typical applications of WSNs include deployment in polluted and hazardous area, difficult to reach places or very extensive fields. For this reason, repairing and restoring exhausted or broken sensor nodes, if at all possible, is not always the best cost effective solution. Energy harvesting WSNs come to a great help in these situations. This explains the increasing attention they are receiving, in terms of development, production and scientific research. Indeed, one of the major limitations of regular WSNs with batterypowered nodes is finite battery capacity, which means nodes operate for a finite amount of time, only as long as the battery lasts. Finite node lifetime implies finite lifetime of the WSN applications or additional cost and complexity to regularly change batteries. Indeed, batteries cannot easily be replaced, since typically WSNs consist of hundreds to thousands of sensors and may be deployed in unreachable places, such as mountains or underground. To make matters worse, depleted batteries constitute environmental problems.

Energy HarvestingWireless Sensor Networks (EH-WSNs) can provide a solution to this problem by harvesting energy that already exists in the surrounding environment. EH-WSNs are wireless sensor networks constituted by nodes that have the special capability of recovering some of the energy surrounding them. This harnessed energy is then converted into electrical energy used to power a node. If the harvested energy source is large and continuously (or periodically) available, a sensor node can be powered perpetually. In this way, energy is essentially infinite; however, not always available. Another important element that differentiates EH-WSNs from classical WSNs is that in EH-WSNs some sensor nodes can be more capable than others. This

is due to the lack of uniformity in the distribution of the harvested energy. As an example, consider a solar-based EH-WSN where some nodes are covered by shadows while others are under direct sun light. In such environment, the more capable nodes can be used to perform energy intensive tasks, on behalf of the incapable nodes that need to sleep and recharge.

As described in [16] we either have the Harvest-Use architecture, where the harvested energy is instantly used to energize the node, or the Harvest-Store-Use architecture, 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, such additional components have an impact on the final cost of the nodes.

Harvestable sources can vary according to their provenance, 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.

3. Security Challenges for EH-WSN

Very interesting and challenging aspects of WSNs are security applications. The data obtained and conveyed through a WSN could be confidential, its integrity could be crucial, or again availability of a given service could be of extremely high importance. 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 [11], [15], [12]. Specific protocols have been designed to secure different aspects of a WSN.

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 nodes. 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 sensor network and so specifically designed approaches are required. While it is obvious that the attacks possible on EH-WSNs are a superset of the one possible for regular WSNs, it is not clear if and how they behave differently, or if new specific attacks can be deployed.

In the following Sections we will introduce a taxonomy of attacks for EH-WSNs and analyze them in order to describe new aspects introduced by the energy harvesting feature.

3.1 Taxonomy of Attacks

In this Section we provide a classification of attacks in WSNs by defining and exploring three dimensions which the attacker can exploit in order to perform an attack. These dimensions are: (i) Intervention, (ii) Presence and (iii) Time. The last two relate to the space domain and the time span which the attack extends over. *Time* can be: (a) short-span, (b) long-span or (c) multiple-spans. The first two relate to a continuous time interval and the last one to multiple related intervals (e.g. the case of replay attacks). *Presence* is either local, distributed or global. With a local attacker only a small part of the network is endangered. On the other hand distributed and global attackers respectively influence multiple parts of the network or the whole system [3].

Finally Intervention takes into consideration the actions that the attacker can do. This is the most interesting dimension since it identifies the actions the attacker can take against the WSN, thus giving a clear idea of possible attacks. We identified nine forms of intervention, extending the six proposed in [4]:

i. **Destruction:** the attacker can destroy one or several devices

ii. **Eavesdropping:** the attacker can intercept and store messages sent between devices.

iii. **Data Knowledge:** the attacker can acquire the data stored on one or multiple devices (e.g. by dumping the whole memory).

iv. **Disturb/Partial Data Modification:** the attacker can partially modify data on a device (without direct access to the memory).

v. **Full Data Modification:** the attacker can fully modify data stored on a device (with direct access to the memory).

vi. **Reprogramming:** the attacker can reprogram a device.

vii. **Device Injection:** the attacker inserts new devices in the network.

viii. **Energy Reduction:** the attacker can reduce the device energy, or control its depletion rate.

ix. **Energy Control:** the attacker can exploit the energy level of a device in a malicious way.

By looking at the above list, it should result clear that in the energy harvesting scenario the last two elements bring to attack patterns which are slightly different with respect to ordinary WSNs. (viii.) Energy Reduction and (ix.) Energy Control could unveil unforeseen attacker strategies when it comes to exploit crypto implementation, especially in systems where the security policies behave according to the energy available (*see Example* 3 *below*).

Another interesting intervention form, which changes role between EH-WSN and legacy WSN, is node injection. If you think for example about large environment monitoring networks, e.g. fire control in a forest, here node injection is a basic mechanism already native to the network to keep it online. Indeed replacing a node can be very expensive and sometimes difficult, the normal way to do it would be to drop new sensors in the network areas where devices start to run out of battery. Therefore, depending on the new node policies, an attacker could easily inject a new node without being discovered. On the other hand in an EH-WSN, the policy on new nodes would be stricter or even completely different, and therefore it would be more difficult, for an attacker, to inject a new node.

It is worthwhile to observe what follows:

• in general, we consider an attack more difficult when the presence of the attacker scales up from local to global; we assume, actually, that the overhead in coordination is not negligible;

• the difficulty of the attack takes also into consideration the number of atomic actions (defined in the following Section 3.2) the given attack needs to be fulfilled.

A thorough and complete analysis of the combinations between the three dimensions is not within the scope of this paper (due to its complexity and length), however, as we extend the work in [4], the reader can refer to it to better understand the methodology and relations between dimensions. We give now three practical examples about the interactions between dimensions, the first is related to a passive threat, while the second and the third to an active one. For a short survey about attacks on WSNs the reader can refer to [11] and [12].

Example 1. With eavesdropping the attacker aims to gather information about the data exchanged. Assuming encrypted data, a local eavesdropper can only gather limited info. However, if we lift Presence to be either Distributed or Global, the attacker can perform traffic analysis inferring network activity and identifying nodes type (e.g. sensor router or access point) just by looking at the bandwidth or at the source and routes of the data exchanged.

Example 2. Looking at energy reduction and node reprogramming, with a local attacker one could launch a Man- In-The-Middle attack or feed forged data into the network, however with Distributed or Global Presence the attacker could aim at lowering the energy of key nodes, thus forcing data to be routed through a node reprogrammed according to the adversary purposes. With respect to the Time dimension, it just gives the attacker more data to analyze in the first example, and increase effectiveness in the second.

Example 3. In [17] an Energy Harvesting-WSN system for secure and energy preserving communication is presented. Here messages have two properties: (i) Priority: from low to high. (ii) Security: from low to high, with different combinations of properties (e.g. confidentiality, integrity etc.). A message is sent only when the node has the right amount of energy to do it and the highest priority messages are sent first, with the most secure policy possible according to the energy level. Through (ix.) Energy Control an attacker could force high priority and high security messages to be sent with low security instead. Here "*low*" security does not mean "*without*" security, but rather with "*less*" security properties (e.g. integrity, authentication etc.).

Eventually, we avoid arranging the attacker's capabilities into a lattice, as proposed in [3] and refined in [4]. Definitely it is an elegant means for comparing the power of different adversaries, but it does not consider a number of constraints arising in real-world scenarios. First of all, some attacks require physical access to a node (e.g. destruction), whereas others do not. Secondly,

and more subtly, it is not always the case that an attacker able to perform a number of attacks chooses the most powerful one: it looks reasonable that strong attacks have a higher cost than weak attacks, and moreover they could require more time to be carried out with respect to simpler ones. Longer the attack, more are the chances to be detected by the system administrators. Thus, a clever attacker is likely to choose the attack which fulfills his needs with the minimum effort in terms of cost and time.

3.2 Energy Harvesting

In order to better understand attacks and relate them to energy harvesting, we identified a set of *atomic actions*. These are the basic bricks of intervention forms. By modelling attacker's basic actions, analyze how feasible it is to perform them and ultimately combine these actions into intervention elements, we thus get an idea of the complexity of attacks down to their atomic actions. 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 subsets of atomic actions, according to the following list:

- Medium/Channel: listen, inject, intercept, destroy, modify, localize, selective block of destination/source communication links (as in [8]).
- Physical: tamper, switch on/off, reduce energy, destroy.
- Cryptography: break encryption (e.g. key attacks), find key (e.g. SPA, DPA [9]), exploit specific crypto mechanisms (weak random number generator or rekeying methods, side channel attacks).

WSNs devices are typically resource constrained in terms of energy and computation. Considering that performing cryptographic operations has a significant 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 in such systems. With EH-WSN, energy potentially is not an issue anymore, and computation could also be improved (more energy translates into less need for reduced low power computation). This brings a whole new perspective and new possible scenarios for security, such as adaptable security levels, waiting queue for highly confidential data (the device transmits the data when it has the energy to encrypt it, according to the confidentiality level of the 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 dimension 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 it 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, or to force them to be transmitted with a low security level even if the data have also high priority. 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. This characteristics also impact on some common protection schemes, according to which a node that disappeared from the network for a long time has to be consider untrustworthy.

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.

Summarizing, EH-WSNs unveil new challenges for security since they are more dynamic and complex than ordinary WSNs, and while they cope with legacy security threats, they introduce new ones, more subtle and perhaps more insidious.

4. Toward Automatic Verification of Security Properties

In this Section we briefly discuss the relationship between the attacks proposed in Section 3 and the capabilities an adversary is generally assumed to exhibit in security protocol analysis. Exploring the connections and the differences between these worlds, we aim at orienting future efforts towards the development of techniques and tools for automatically verifying security properties of EH-WSNs, on the basis of the successful experience documented in security protocols verification since the late '90s. A formal attacker model is indeed a central factor for devising tools for security analysis, and the capabilities discussed

above introduce new features not yet considered in the literature.

The framework proposed by Benenson et al. in [4], and extended in Section 3.1, is claimed to express well-known attacker scenarios like the Dolev-Yao (formal) model [8], as well as other attackers mentioned in the literature. In particular, they claim that a Dolev-Yao adversary can be represented as combination of a global eavesdropping with a distributed disturbing adversary, that in their general adversary model can be expressed as {(global, eavesdropping), (distributed, disturbing)}.

In order to carry out a more precise comparison between different attacker models we introduce a simple map describing model elements with security protocol standard notions. Each node of a EH-WSN corresponds to an agent of a security protocol, equipped with some knowledge (the memory of the node) and playing a given role (determined by the software controlling the node). The knowledge of a principal is either a priori (e.g. predefined keys) or gained through running the protocol (e.g. session keys). This map can be leveraged for translating the attacker's capabilities proposed by different models in a uniform framework, that enables a less ambiguous comparison. The capabilities discussed in Section 3 translates as follows:

1. destroying a node, the adversary inhibits the corresponding principal to participate in the protocol;

2. reading the memory of a node, the adversary is able to obtain the knowledge of a principal at the attack time;

3. modifying the memory of a node, the adversary is able to modify the knowledge of a principal; this is more powerful than simply sending messages, as it allows to alter information already received;

4. reprogramming a node, the adversary makes the corresponding principal play an arbitrary role in the protocol.

In this way we obtain a simple translation of physical attacks in terms of cyber actions, by looking at their effects. Two main considerations stem from this argument.

First, if the adversary obtains the knowledge of a principal A and he is able to eavesdrop and send messages on the network, then he can impersonate *A* in the protocol. As a matter of fact, the knowledge of a principal defines his identity (e.g. private keys), and thus the attacker can pass off as *A* in the protocol, that is, reprogramming the corresponding node. This implies that a standard Dolev-Yao attacker able also to physically read the memory of a node is capable of reprogramming, with much less effort than the one required by real reprogramming. We can conclude that, from a protocol perspective, *Eavesdropping+ Data Knowledge+Disturb/Partial Data Modification* implies reprogramming. Finally, it is worth noting that reprogramming is the most powerful achievement that an attacker can pursue, thus we can ignore memory writing and reprogramming physical attacks.

Secondly, the translation sketched above does not account for energy related attacks. These involve properties of the principals that have never been considered in standard protocol verification settings, as far as our knowledge is concerned. This is not a shortcoming of the translation, but a limit of state-of-the-art protocol formalization pointed out by the new capabilities of our attacker.

The comparison with the standard Dolev-yao model is now straightforward: such an attacker is not able to fully simulate the cyber effects of physical attacks, but he is limited to get outputted knowledge and modify a principal's knowledge by inserting new messages. What is more, a Dolev-Yao attacker is generally assumed to access the whole system, i.e. he is global. Clearly, this assumption is not always suitable when dealing with EH-WSNs, whose dimension can scale up to thousands of nodes scattered through a wide area.

The physics-aware attacker proposed by Basin et al. [1] plug the gap of the spatial specification of the attacker, allowing also to reason about temporal properties. On the capabilities side, however, the authors refer to a Dolev-Yao adversary.

A more powerful though global adversary is proposed in [2], where the notion of agent compromise is introduced for modelling the event in which the attacker obtains secret data of a given principal. This capability closely models a *Data Knowledge* attack, the only element a Dolev-Yao attacker lacks for implementing a reprogramming adversary. Nonetheless, the adversary defined in [2] is explicitly prevented from obtaining session keys, and the authors state that it is unclear whether any protocol would be secure with respect to a fully compromising adversary.

This consideration highlights another novelty that EH-WSN (and Cyber-Physical Systems, more in general) brings into computer

security: the capabilities of a cyber-physical attacker allow for breaching any system. Nonetheless, such an attacker is hampered by spatial, temporal, and energy constraints, that must be considered when analysing the security of a system with respect to such an attacker, otherwise we would always be told that system is insecure. This calls for a quantitative approach in security verification as opposed to the standard qualitative approach on which most of the security protocol verifiers are based (see, for example, [6]). Some efforts have already been devoted to devise tools which perform quantitative analyses, like [5], and EH-WSN security verification pertains to this second line of research.

Since we cannot extract meaningful information about the attacks to which a EH-WSN is exposed without modelling some of the parameters that constrain the adversary, extending available tools with energy and spatial reasoning seems a promising direction for future investigation.

5. RelatedWork

We will now describe the state of the art for security specific solutions in the EH-WSN field. Being this a fairly recent topic, only two interesting approach can be found in literature. In both cases an adaptive security mechanism is presented, even though the actual approach is somehow complementary.

5.1 Strength Oriented Approach

The first energy harvesting specific approach for security that we are going to describe is the one presented in [17]. 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, the energy overhead introduced by cryptography, the energy wasted due to channel errors, etc.

The main idea is to provide a list of possible priority levels and supported security suites with different characteristics and parameters. 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 a higher overhead for the transmission, which translates into a 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.

The optimization process works with a threshold value defined as the amount of energy that can be consumed to send packages in a given time slot. The specific policy proposed in the paper starts by selecting all the packets above a given priority level in order to form an outgoing queue, and calculating the amount of energy needed to send them. If this value is within the limit, the security suite chosen for every package in the queue is improved as much as possible according to the available choices. On the other hand if the amount of energy required to process the queue is above the threshold, then the most energy demanding packets are removed from it.

5.2 Time Oriented Approach

The second solution that we are going to analyze is [14]. It takes a completely different approach. Here 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. Starting from here, the authors suggest precomputing and storing keystream bytes in a buffer, and use them when the energy within the system is scarce.

To find out if the system can work correctly under given conditions they assume the existence of a power management system that, for every round of execution, chooses a duty cycle. The active time of a node is then compared to a threshold, if the value is below it the node can only do its operations but not calculate and buffer the keystream bytes. If the active time is above such threshold then the node can do both operations. For the system to correctly run over a given number of rounds, in every round a node should extract less bytes than those available in the buffer. Furthermore, the node should make sure that at the end of every round its buffer contains at least as much data as what is going to be used in the next round. This can be achieved by not

removing a big enough number of bytes, or by storing new ones (only if the duty cycle allows it). In the paper it is also suggested a very basic model for computing the buffer size. Supposing a periodic function for the activity, the node is allowed to store keystream bytes only at the beginning of the period. Then, for the whole system to run properly the size of the buffer should be at least as big as the amount of data that the node will transmit in the remaining portion of the period. 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 presented work also introduces the possibility of having, beside encryption, authentication capabilities. To do so the authors implement a Wegman-Carter MAC scheme [7] based on the Poly32 universal hash function family [19].

5.3 Discussion

The first proposed approach directly takes advantage of the inherent properties of EH-WSNs by implementing a security system that adapts itself according to the amount of energy available in a given node and an external constraint for the maximum energy consumption allowed that can be tuned to enhance security performances over node's lifetime and vice versa. Within these limits the proposed model successfully applies the strongest available security suite and guarantees a 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. Even if we still consider the case where traffic only moves from the nodes to the link there are going to be nodes out of the sink's direct reach that will have to relay their messages to other nodes. 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 [10], 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, 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. As briefly mentioned in the future work section of the paper, an interesting idea could be the one of relying 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.

6. Conclusion and Future Work

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 analyzed how well known attacks for WSNs change in the energy harvesting domain. As a result, we proposed a first threat model for EH-WSNs.

Moreover, we sketched how EH-WSNs security issues can be described with terminology coming from the protocol verification world. The benefit of the conceptual map we drew is twofold. On one hand, it opens up for the exploitation of formal methods,

successfully used for security protocols analysis, in the verification of WSNs security properties. On the other hand, it highlights that state-of-the-art protocol verification framework cannot deal with the cyber-physical attacker, sketching thus a line for future work in both directions.

Finally, we 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. As remarked in the paper, security in EH-WSNs represents a very young research field so that not many interesting solutions have been discovered yet. To the best of our knowledge these approaches are the only two that perfectly match the topic of interest. Anyway we think that this is the right path to follow for future research in this domain. 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 appealing feature to have.

Many EH-WSNs applications require different network typologies or traffic shapes, so extending such solutions to those scenarios constitutes the next natural research step.

References

[1] Basin, D., Capkun, S., Schaller, P., Schmidt, B. (2011). Formal reasoning about physical properties of security protocols, *ACM Transactions on Information and System Security* (*TISSEC*), 14 (2) 16.

[2] Basin, D., Cremers, C. (2010). Degrees of security: Protocol guarantees in the face of compromising adversaries. *Computer Science Logic*, p. 1–18. Springer.

[3] Benenson, Z., Dewald, A., Freiling, F. C. (2008). Vulnerabilities and Attacks in Wireless Sensor Networks. *Wireless Sensors Networks Security*. IOS Press, (Cryptology & Information Security Series).

[4] Benenson, Z., Dewald, A., Freiling, F. C. (2010). Presence, Intervention, Insertion: Unifying Attack and Failure Models in Wireless Sensor Networks.

[5] Blanchet, B. (2007). Computationally sound mechanized proofs of correspondence assertions. *In: Computer Security Foundations Symposium*. CSF'07. 20th IEEE, p. 97–111. IEEE.

[6] Blanchet, B. (2009). Automatic verification of correspondences for security protocols. *Journal of Computer Security*, 17(4) 363–434.

[7] Lawrence Carter, J., Wegman Mark, N. (1977). Universal classes of hash functions (extended abstract). *In*: Proceedings of the ninth annual ACM symposium on Theory of computing, STOC '77, p. 106–112, New York, NY, USA. ACM.

[8] Dolev, D., Yao, A. (1983). On the security of public key protocols, *IEEE Transactions on Information Theory*, 29 (2) 198–208.

[9] Kocher, P., Jaffe, J., Jun, B. (1999). Differential power analysis. In Advances in Cryptology - CRYPTO'99, p. 789–789. Springer.

[10] Jun Lu, Shaobo Liu, QingWu, Qinru Qiu. (2010). Accurate modeling and prediction of energy availability in energy harvesting real-time embedded systems. *In:* Green Computing Conference, International, p. 469–476, aug.

[11] Lupu, T. G., Rudas, I., Demiralp, M., Mastorakis, N. (2009). Main types of attacks in wireless sensor networks. *In*: WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering, WSEAS.

[12] Martins, D., Guyennet, H. (2010). Wireless sensor network attacks and security mechanisms: A short survey. *In:* Network-Based Information Systems (NBiS), 13th International Conference on, p. 313–320, sept.

[13] Di Mauro, A., Papini, D., Vigo, R., Dragoni, N. (2012). Toward a threat model for energy-harvesting wireless sensor networks. *In*: Proc. Networked Digital Technologies 4th Internation Conference (NDT 2012), p. 289–301, Dubai, UAE, April.

[14] Pelissier, S., Prabhakar, T. V., Jamadagni, H. S., VenkateshaPrasad, R., Niemegeers, I. (2011). Providing security in energy harvesting sensor networks. *In:* Consumer Communications and Networking Conference (CCNC), IEEE, p. 452–456, jan.

[15] Jaydip Sen. (2010). A survey on wireless sensor network security. CoRR, abs/1011.1529.

[16] Sudevalayam, S., Kulkarni, P. (2011). Energy Harvesting Sensor Nodes: Survey and Implications. *Communications Surveys Tutorials, IEEE,* 13 (3) 443–461, quarter.

[17] Antonio Vincenzo Taddeo, Marcello Mura, Alberto Ferrante. (2010). Qos and security in energy-harvesting wireless sensor networks. *In*: Security and Cryptography (SECRYPT), *In*: Proceedings of the 2010 International Conference on, p. 1–10, july.

[18] Wander, A. S., Gura, N., Eberle, H., Gupta, V., Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. *In*: Pervasive Computing and Communications. PerCom . Third IEEE International Conference on, p. 324–328, March.

[19] Dongho Won, editor. (2001). Information Security and Cryptology - ICISC 2000, Third International Conference, Seoul, Korea, December 8-9, *In*: Proceedings, V. 2015 of Lecture Notes in Computer Science. Springer.