A SECURITY FRAMEWORK FOR A 6LoWPAN BASED INDUSTRIAL WIRELESS SENSOR NETWORK

Ionela HALCU[1], Grigore STAMATESCU[2], Valentin SGÂRCIU[3]

This paper proposes a security framework solution in the context of Industrial Wireless Sensor Networks (IWSN). A particular focus is put on the usage of IPv6 networks, based on a number of security challenges associated with industrial applications. The paper also presents potential architectures configurations for monitoring applications to overcome the security challenges. Leveraging the Contiki operating system for resource constrained devices, along with link-layer security sublayer and 6LoWPAN, helpful insight is achieved for evaluation and deployment.

Keywords: WSN, IWSN, 6LoWPAN, link-layer security, Contiki

1. Introduction

Industrial Wireless Sensor Networks (IWSN) are an emerging area of Wireless Sensor Networks (WSN), with specific constraints related to the particularities of industrial automation systems. The design and deployment of Industrial Wireless Sensor Networks are extremely challenging tasks. The most current challenges in IWSN are related to the dynamic environment where IWSNs are deployed, the operation lifetime, heterogeneity, autonomous operation, maintainability, reliability and security [1].

Security is one of the main challenges in IWSN. The concept of security can refer to the information that flows throughout the system, the products and equipment, or the security of people. In our study, we focus on securing the real-time information provided by the network. For relevant goals, we consider security should properly be addressed as an integral part of both low-level and high-level layers of the protocol stack. Possible threats present in an IWSN include: disclosure of sensitive/confidential data, Denial of Service (DoS) attacks, unauthorized access to wireless-enabled resources, potential weakening of existing security measures on connected networks and systems.

[1] PhD student, Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania, e-mail: halcuionela@gmail.com

[2] Prof., Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania

[3] Prof., Dept. of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania

Nowadays, there is a trend to use the IPv6 protocol within the WSN area. It is important to determine if recent development of IPv6 based wireless networks (e.g., 6LoWPAN, SNAP) are suitable for IWSNs. These protocols are primarily intended for home automation and not industrial applications. The main question with IP based wireless protocols is if the large protocol overhead can be justified in an industry setting. It is important for commercial development of IWSNs to provide services that can be accessed remotely from the Internet, and hence, need to be integrated with the IP protocol [2].

In our previous research, we analyzed the communication and security constraints in a 6LoWPAN-based WSN [3] and we focused on the implementation of a link-layer security solution for a 6LoWPAN network [4]. In this paper, we approach the IWSN application context, with specific constraints (e.g. interoperability, reliability, standardization) over general IPv6-based WSNs. In this paper, our aim is to provide an inside of the security challenges present in IWSNs and to define a framework for utilization in IWSN applications.

The main contribution of this work is to provide a security solution based on selected hardware and software instruments in an IWSN system design. The proposed framework enables the protection of IPv6 packets within IWSNs. The security extensions are defined considering the challenges, characteristics and design principles of an IWSN. When designing new algorithms, protocols and communication architectures for IWSNs, a proper analysis on the performances, energy usage and interoperability must be done. We validate the usage of the security extensions in terms of network performance and computational requirement from measurements obtained experimentally. We believe that our proposal can give a valid contribution towards the adaptation of security in a 6LoWPAN IWSN context.

The structure of this paper is organized as follows. Section 2 defines the characteristics of IWSNs. In section 3, we identify the security challenges present in regular IWSNs, followed by the proposed security framework for a 6LoWPAN IWSN. Analysis of the solution is presented in section 5. Section 6 concludes the paper.

2. Industrial Wireless Sensor Networks

In this section, we discuss the applications of WSNs in industrial environments. Based on the specific requirements of the industrial production, the IWSN applications can be divided into three different application domains [5]:

1. **Environmental sensing**. IWSN applications for environmental sensing include pollution of air or water, environmental hazards and security issues where IWSNs are used for point of interest, area and

barrier monitoring. Nowadays, this kind of applications are generally the widest field of WSN.

2. **Condition monitoring.** This group covers the problems of structural health (condition of buildings, bridges, constructions, etc.) and equipment condition, and human condition monitoring (healthcare applications).
3. **Process automation**. This group of applications include evaluation and improvement of industrial processes that can be achieved through IWSNs.

IWSNs support heterogeneous industrial applications with different requirements. It is necessary to develop flexible and scalable architectures that can overcome all the requirements in one infrastructure [2]. A general architecture of an IWSN is illustrated in Fig.1.

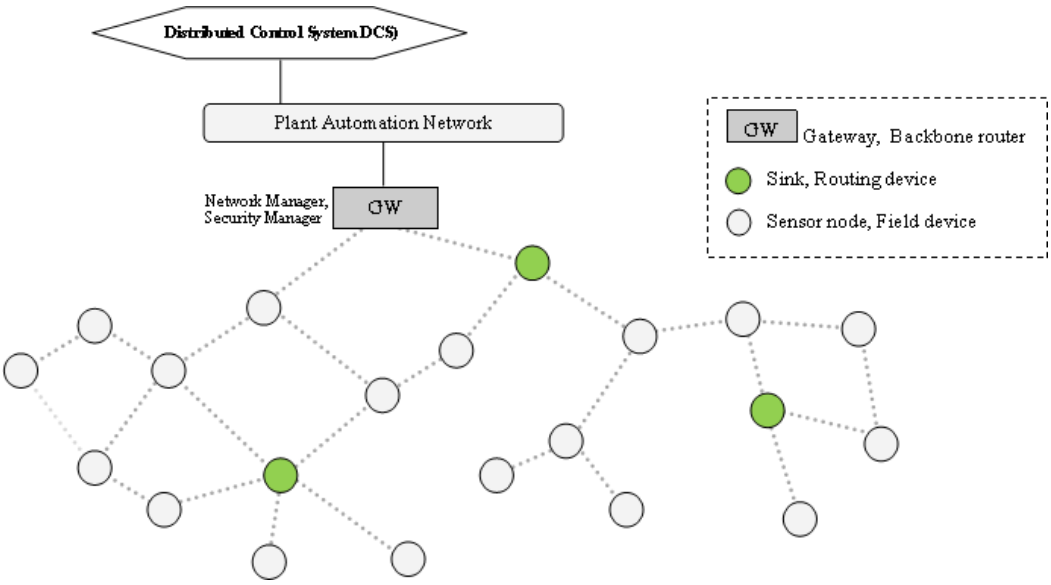

Fig. 1 A general industrial wireless sensor network system architecture

2.1 Challenges in IWSNs

Environmental conditions. Due to harsh environmental conditions and dynamic network topologies, industrial sensor nodes failures or intermittent connectivity may be present [5]. Furthermore, sensors can be subject to medium interferences, high humidity or temperature levels, noise, dirt, or other conditions that challenge the network performance.

Quality-of-service (QoS). QoS requirements and specifications are highly dependent on the application envisaged on IWSN. Some applications may be

time-sensitive, and long latency due to communication or processing issues may lead to severe consequences in the monitoring system. The QoS provided by IWSN refers to the accuracy between the sensing data and what is reported to the control center (the sink node).

Deployment. Most IWSNs contain hundreds or even thousands of sensor nodes which may be spread randomly across the deployment field. Moreover, the lack of a network infrastructure necessitates IWSNs to establish and maintain network connectivity autonomously.

Resource constraints of sensor platforms. There are three types of constrained resources in an IWSN context: energy, memory and processing.

Topology changes, packet errors and link capacity. Compared to wired networks, in IWSNs, wireless links are subject to obstructions and noisy environment. The attainable capacity of each wireless link depends on the interference level perceived by the receiver, resulting high bit error rates [5].

Integration issues and security. When designing an IWSN, security should be an essential feature, as more and more attacks and intrusions can compromise the communication and operability of the network. Although today's sensor networks use gateways for integration between IWSNs and the Internet, IPv6 offers the possibility for remote access of every sensor nodes.

2.2 Standards for IWSNs

Since industrial automation has specific requirements compared to the consumer industry, specific wireless communication standards are required. There are different standards suitable to each industrial application [6]. Most recently standardization efforts for wireless communication in industrial automation are: ZigBee, WirelessHART, ISA100.11a, and IETF 6LoWPAN. They are all based on the IEEE 802.15.4 physical layer.

3. Security Challenges in Industrial Wireless Sensor Networks

In general, security issues are not handled independently, a tradeoff with usability and performance needs to be addressed [2]. Sensor nodes are resource-limited devices and some of them might be mobile. This mobility requires re-authentication. Additionally, the industrial application may require that sensor nodes should be privacy protected. All these concerns should be addressed by the proposed security solutions intended for the IWSN. The security challenges associated with IWSNs can be outlined as follows:

Resource Constraints. Sensor nodes are resource-constrained devices in terms of battery life, CPU capability, and memory capacity. Enabling IWSNs with security may increase the overhead in sensor node resource consumption. In [7], we determined that energy consumption highly depends on the employed MAC

protocol. Security protocols should be built requiring limited bandwidth (e.g., reduced number of exchanged messages, small packet size) and using low-cost cryptographic primitives (e.g., symmetric cryptographic algorithms, hash algorithms).

Scalability. Since sensor nodes are deployed as low-cost and small devices, in large scale and densely within the IWSN, the load of security overhead should be distributed across the network. The network must be organized into clusters and sub-divisions of clusters.

Mobility Support. Some industrial applications may require sensor nodes to be mobile. Nodes may move within the same IWSN or to another IWSN. In this case, the security solutions should support cross-domain capability.

Intermittent Connectivity. IWSNs have generally dynamic network topologies due to potential node breakdown or mobility. Moreover, some nodes may fail due to error-prone wireless medium, battery depletion, or sensor node failures, which results in unreliable communications between sensor nodes and the application infrastructure.

Privacy. Privacy protection becomes more and more an important issue in industrial applications, particularly if sensor nodes move across different administrative domains. Sensor nodes may handle sensitive data and contextual information (e.g., worker/consumer identity, location) that should be kept secret to the outside world. Security protocols should have built-in privacy-preserving techniques.

4. Bringing security to IWSN

In this chapter, we focus on the implementation of a security sublayer in an IEEE 802.15.4-based industrial wireless sensor network. To do so, we need to take into consideration the specific requirements of a typical IWSN application. In Table 1, the factors that influence designing of IWSNs are outlined, also with the design goals that need to be followed.

When designing security mechanisms for IWSNs, the security primitives must be addressed for both low-level and high levels of the protocol stack. For example, key establishment and trust management, authentication, privacy, secure routing, integrity protection, DoS prevention, resilience to compromised nodes, etc. are one of the many tasks security should cover. In addition, the security overhead should be balanced against all other requirements, because of resource limitations of IWSNs. Within this context, the task of the sensor network designer is first to choose among a range of available algorithms, protocols and platforms which build up a complete system, while using widely accepted hardware and software tools [2].

Table 1

Factors influencing IWSN's design

Factor		Design goals
Fault tolerance and deployment		Reliability, self-configuration and self-organization
Scalability		Adaptive scalability
Cost		Low cost and small sensor nodes
Power consumption		Resource efficient design
Hardware and software constraints		Application-specific design
Topology maintenance		Adaptive network operations
Quality of service		Real-time performance
Security		Secure design
Transmission media		Interoperability and scalable architectures

The following architecture (Fig. 2) is a proposal of selected instruments for a secure design of environmental sensing application or conditional monitoring IWSN application. The selection of protocols is based on energy-efficiency, accuracy, latency and time-synchronization requirements.

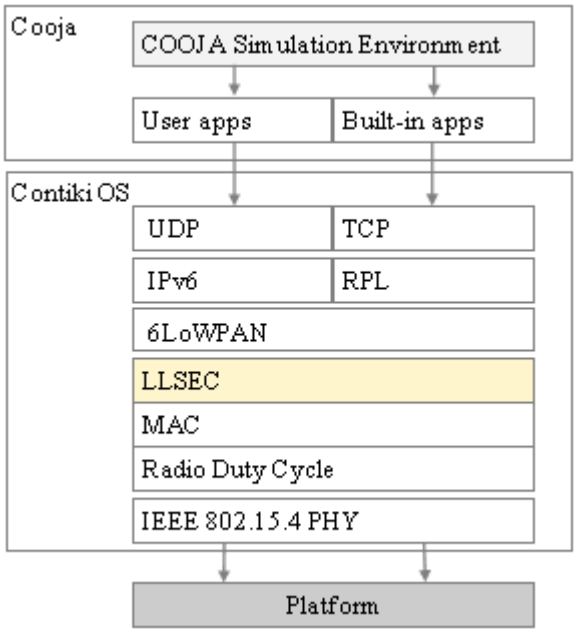

Fig. 2 Proposed architecture with link-layer security (LLSEC)

Contiki [8] is a lightweight operating system for resource constrained devices, also called the open-source OS for the Internet of Things (IoT). Contiki

runs on a range of different hardware platforms and is designed to be easy to port to new hardware. It has a very small memory footprint, a typical system can run with less than 10K of RAM and 30K of ROM. To assist the development of low-power systems, Contiki provides mechanisms for estimating the system power consumption and for understanding where the power was spent. In addition, Contiki provides a full IP network stack, with standard IP protocols such as UDP, TCP and HTTP, including support for new low-power standards and IPv6 networking, like 6LoWPAN, CoAP, RPL etc. In the current Contiki version, there are no existing key distribution protocols and security service layer implemented. Various proposals have been made recently in [9][10][11]. A security layer should be implemented in Contiki to provide the basic security services, including encryption/decryption and authentication. A suitable key management scheme is also needed to support both hardware-based and software-based security.

The Tmote Sky hardware platform we chose is one of the most popular WSN platforms under Contiki OS, used in sensor networks, monitoring applications and rapid application prototyping. The Tmote Sky specifications are: the 16-bit MSP430 MCU, 10 kB of RAM, 48 kB of ROM, the CC2420 802.15.4 radio transceiver, an external flash memory, and various sensing elements [12]. We chose this platform as a low-cost, low power consumption hardware solution to test the performances of our security-based architecture. Tmote Sky enables a wide range of mesh network applications and it is also energy-efficient [13].

The IEEE 802.15.4 MAC layer provides access control to a shared channel and reliable data delivery. In low-power networks, the radio transceiver must be switched off as much as possible to save energy. This is strongly recommended for battery operated applications. In Contiki, low power consumption may be achieved by the Radio Duty Cycling (RDC) layer. The configured RDC and MAC protocols for our Contiki project are ContikiMAC and CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance).

The link-layer security sublayer (LLSEC) is a new compressed header for Contiki stack. This sublayer widely depends on the existing IEEE 802.15.4 security mechanisms and supports pairwise keys so as to mitigate node compromises. We consider that this security sublayer fit in an IWSN context, because it offers energy-efficiency and DoS resilience [9]. First, we need to choose a pairwise key establishment scheme, which is adaptable to different 6LoWPAN networks and threat models. The key establishment we used is the one proposed in [9], namely Adaptable Pairwise Key Establishment Scheme (APKES). Its role is to establish pairwise 802.15.4 session keys with neighboring nodes. Different key pre-distribution schemes can be configured for APKES to adapt to different 6LoWPAN networks (e.g. LEAP, fully pairwise scheme, random scheme). Second, an easy-to-implement and compromise-resilient protocol for authenticating broadcast frames is used. Together, these add-ons

detect compromised nodes, prevent all known WSN attacks and is energy-efficient. Beyond that, LLSEC prevents unauthorized nodes from joining a 6LoWPAN network.

The 6LoWPAN (IPv6 over Low power Wireless Personal Area Network) protocol stack [14] offers fragmentation and header compression mechanisms that allow the transmission of IPv6 packets over IEEE 802.15.4 based networks. 6LoWPAN aims for standard IP communication over low-power wireless IEEE 802.15.4 networks utilizing IPv6 protocol. From the industrial point of view, the advantages of 6LoWPAN are ability to communicate directly with other IP devices locally or over the IP network (e.g., Internet, Ethernet), existing architectures and security, established application level data model and services (e.g., HTTP, HTML, XML), established network-management tools, transport protocols, and existing support for an IP option in most industrial wireless standards. On layer 3, the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [15] routes the IPv6 packets.

The vulnerabilities of a 6LoWPAN stack without the 802.15.4 security sublayer are present both in low-levels and high-levels of the network stack. For e.g., attackers can inject replay frames at layer 2, fragmentation attacks at layer 2.5, path-based DoS (PDoS) at layer 3, and so on. To prevent these attacks, and to prevent injection and replay attacks in general, LLSEC authenticate each neighbor and has the ability to detect and discard non-authenticated frames. As an alternative to the 802.15.4 security sublayer, mitigation mechanisms against known fragmentation attacks are proposed [16], also with mechanisms for RPL routing protocol [15]. However, these security mechanisms are focused on specific attacks and introduce complexity, leaving other threats unhandled. The 802.15.4 security sublayer protects against all these attacks at once, therefore is more efficient.

5. Experiment setup and test results

Our study evaluates the feasibility of employing the proposed scheme according to the security requirements of IWSNs presented in section 3. To prove that the security solution work in real industrial scenario and that the system meets the application-specific requirements, we conducted the experiments in Contiki/Cooja WSN network simulator [8]. Cooja is based on real hardware emulation and time-accurate WSN simulation. It can emulate the Tmote Sky nodes (among other WSN platforms) and to connect them. The code executed on the node is the exact firmware that runs on the physical node.

To show the feasibility and performance of the security sublayer, we test a network with 46 sensor nodes, both with and without encryption enabled. The

parameters used for simulation are based on the Tmote Sky hardware, as shown in Table 2.

Table 2

Simulation parameters used in Cooja

Simulation parameters	Default value
Hardware	Tmote Sky
Transmit power	36.23 mW
Radio propagation model	Undirected graph model
Inter-packet arrival time	10 seconds
MAC protocol	CSMA-CA
RDC protocol	ContikiMAC
MAC layer queue size	30 packets
Channel bandwidth	250 Kbps
Node transmission range	50 meters
Node carrier sensing range	100 meters
Total frame size	127 bytes

Since the topology design algorithms produce different solutions, we need to simulate a network protocol in the presence of node failures to show the robustness of the design. An example of a simulated IWSN topology is illustrated in Fig. 3.

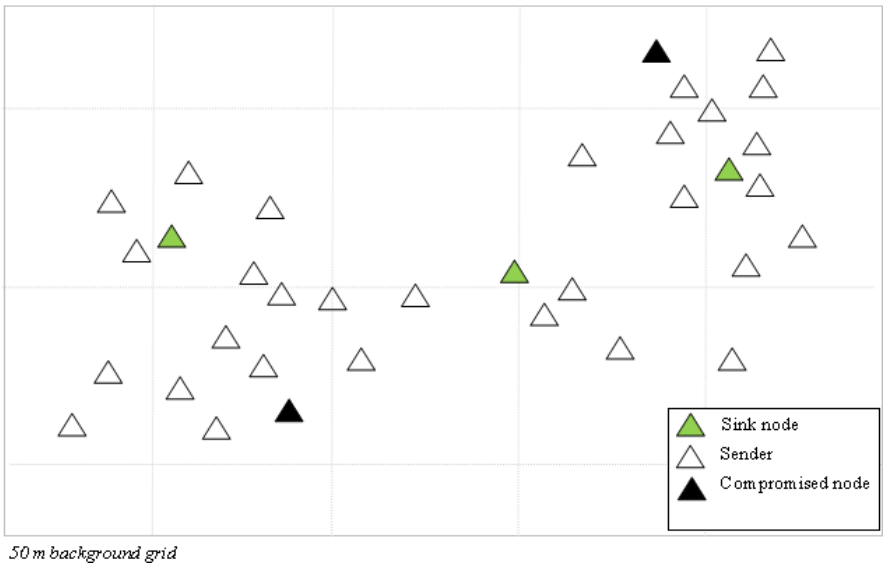

Fig. 3 Example of simulated network topology

The sensor nodes (senders) generate packets and send them to the authenticated neighbors. They also forward the packets of other nodes toward the

sink. The sink node act as a gateway between the 6LoWPAN network and the Internet or the plant automation network. We use the following metrics for the evaluation of network operations, relevant to the evaluation of security: packet delivery ratio, average per packet latency and completeness of packets received. Experimental results collected are shown in Fig. 4-9.

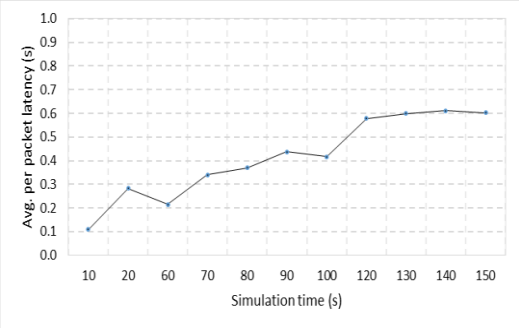

Fig. 4 Latency in time simulated network

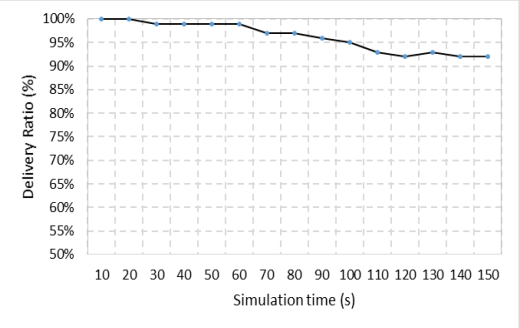

Fig. 5 Delivery ratio in time

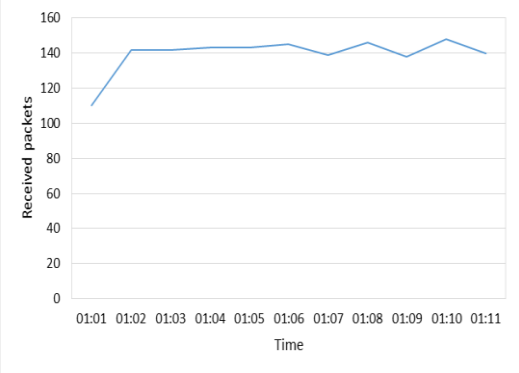

Fig. 6 Number of received packets over time

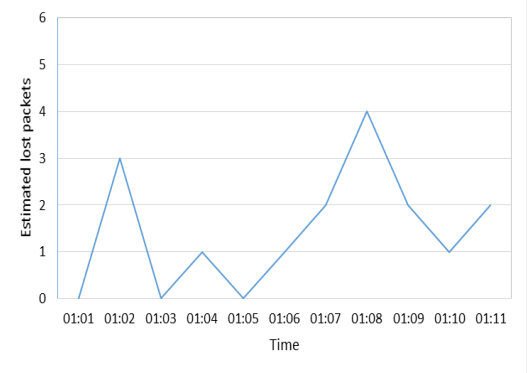

Fig. 7 Estimated number of lost packets over time

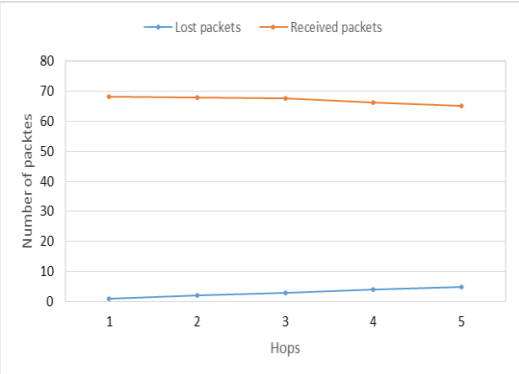

Fig. 8 Successfully delivered packets and lost packets over the number of hops

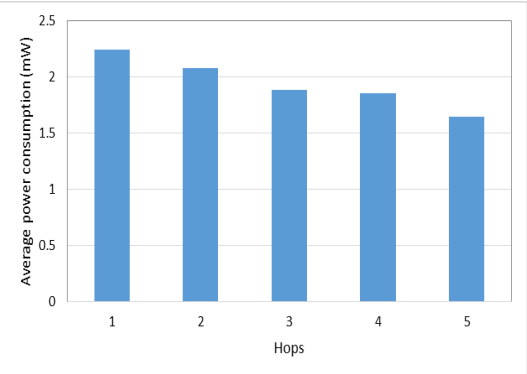

Fig. 9 Average power consumption, hop dependent

The results presented are based on the topology simulated during 705 seconds, where all sensor nodes generate packets within fixed intervals (10s).

In Fig. 4, we performed an experiment to measure the end-to-end latency for data packets sent between sensor nodes and sink node in the network. Fig. 5-7 depicts the number of successfully transmitted packets and the estimated number of lost packets under given configuration. The throughput of the network is calculated as 4 packets/s. All data packets has a 30 byte payload. The radio needs to transmit a total of 103 bytes per data frame. The average power consumption depending on the number of hops present in the network is shown in Fig. 9.

Experimental results show that our framework implementation on an IWSN application provide efficient network convergence (44s), control traffic overhead (2841 packets), energy consumption (15% radio on-time), latency (0.41s), packet delivery ratio (96%) in our sample simulation with 46 nodes, after careful configuration of transmission range, link success rate (>85%), radio duty cycling, and frequency of application messages. The 85% radio sleep time is due to the ContikiMAC mechanism used in all simulations.

6. Conclusions

In this paper, we propose and simulate a security framework in the context of IWSNs with the aim to study their integration into industrial applications. We discuss the applicability in the industrial domain based on a number of derived security challenges associated with this type of applications. The proposed framework is flexible, configurable, and has the potential of adapting to the challenges of wireless monitoring and control in industrial environments.

We analyze and implement link-layer security headers for 6LoWPAN networks, together with well-known protocols for WSNs. We conduct performance analyses for the protocol design and propose corresponding countermeasures with the support of the implemented framework.

We envision providing secure real-time services over motes, transparent to the application layer, to integrate industrial applications into the Internet. This integration can bring benefits to the development of IWSNs, e.g. retrieving useful information from anywhere at any time.

Acknowledgments

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132397.

REFERENCES

[1]. *V. C. Güngör, G. P. Hancke,* Industrial Wireless Sensor Networks: Applications, Protocols and Standards, CRC Press, Series Industrial Electronics, USA, 2013.

[2]. *V. C. Güngör, G. P. Hancke,* "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches", IEEE Transactions on Ind. Electronics, **vol. 56**, no.10, Oct. 2009, pp. 4258-4265.

[3]. *I. Halcu, G. Stamatescu, I. Stamatescu, and V. Sgarciu*, "An analysis of security and communication constraints of IPv6-based Sensor Networks," in Proceedings of the 2014 6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2014, pp. 55–60.

[4]. *I. Halcu, G. Stamatescu, V. Sgarciu*, "Enabling Security in 6LoWPAN/IPv6 Wireless Sensor Networks", in Proceedings of the 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2015, pp. 29–33.

[5]. *Gang Zhao*, "Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey", in Network Protocols and Algorithms, **vol. 3**, no. 1, Feb. 2011, pp. 46-63

[6]. *Radmand, P.; Talevski, A.; Petersen, S.; Carlsen, S.,* "Comparison of industrial WSN standards," in Digital Ecosystems and Technologies (DEST), on 2010 4th IEEE International Conference, pp.632-637, 13-16 April 2010

[7]. *M.O. Farooq and T. Kunz*, "Contiki-based IEEE 802.15.4 node's throughput and wireless channel utilization analysis," IFIP Wirel. Days, pp. 3–5, 2012.

[8]. *A. Dunkels, N. Eriksson, F. Österlind, and N. Tsiftes*, "The Contiki OS - The Operating System for the Internet of Things." [Online]. Available: http://www.contiki-os.org/.

[9]. *K.-F. Krentz, H. Rafiee, and C. Meinel*, "6LoWPAN security: Adding Compromise Resilience to the 802.15.4 Security Sublayer," Proc. Int. Work. Adapt. Secur. - ASPI'13, pp. 1–10, 2013.

[10]. *J. Granjal, E. Monteiro, and J. S. Silva*, "Enabling Network-Layer Security on IPv6 Wireless Sensor Networks," 2010 IEEE Glob. Telecommun. Conf. GLOBECOM 2010, pp. 1–6, Dec. 2010.

[11]. *S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt*, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," Secur. Commun. Networks, **vol. 7**, no. 12, pp. 2654–2668, Dec. 2014.

[12]. *** Tmote Sky Datasheet, available at: www.eecs.harvard.edu/.../tmote-sky-datasheet.pdf

[13]. A. *Dunkels, J. Eriksson, N. Finne, and N. Tsiftes*, "Powertrace : Network-level Power Profiling for Low-power Wireless Networks Low-power Wireless," in SICS Technical Report T2011:05, 2011.

[14]. *G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler*, "Transmission of IPv6 packets over IEEE 802.15.4 networks," Internet Engineering Task Force RFC-4944, Sept. 2007.

[15]. *T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander*, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," 2012.

[16]. *R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle,* "6LoWPAN fragmentation attacks and mitigation mechanisms," in Proceedings of the sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '13, 2013, p. 55.