A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication

Michael Heigl[*†], Martin Schramm[†] and Dalibor Fiala[*]
[*]University of West Bohemia, Pilsen, Czech Republic
Email: {heigl, dalfia}@kiv.zcu.cz
[†]Deggendorf Institute of Technology, Deggendorf, Germany
Email: {michael.heigl, martin.schramm}@th-deg.de

***Abstract*—The ubiquitous internetworking of devices in all areas of life is boosted by various trends for instance the Internet of Things. Promising technologies that can be used for such future environments come from Wireless Sensor Networks. It ensures connectivity between distributed, tiny and simple sensor nodes as well as sensor nodes and base stations in order to monitor physical or environmental conditions such as vibrations, temperature or motion. Security plays an increasingly important role in the coming decades in which attacking strategies are becoming more and more sophisticated. Contemporary cryptographic mechanisms face a great threat from quantum computers in the near future and together with Intrusion Detection Systems are hardly applicable on sensors due to strict resource constraints. Thus, in this work a future-proof lightweight and resource-aware security concept for sensor networks with a processing stage permeated filtering mechanism is proposed. A special focus in the concepts evaluation lies on the novel Magic Number filter to mitigate a special kind of Denial-of-Service attack performed on CC1350 LaunchPad ARM Cortex-M3 microcontroller boards.**

I. Introduction

A Wireless Sensor Network (WSN) consists of individual interconnected sensor nodes, which collect data from the immediate environment and transmit them via wireless communication to their neighbours and base stations. Typical application areas are environmental data (climatic measurements, presence of smoke), health (measurement of vital signs, body temperature) or home automation (motion sensor and image sensor) [1]. Every sensor device is powered by a battery and equipped with a radio transceiver. These systems are finding their way into more and more areas mainly driven by the Internet of Things (IoT). For example, with intelligent transportation leveraging features and capabilities from WSN, IoT-enabled Smart Cars can be designed [2]. The rise and success of cryptocurrencies based on Distributed Ledger Technologies, e.g. IOTA, even creates a monetary system allowing micro- and nanopayments between IoT-devices [3]. Considering the internetworking of a large quantity of intelligent nodes, the phrase Smart Dust inspires the WSN-trend.

The need for security in WSN, which arises from the transmission of security-relevant information and for maintaining the functionality of the WSN cannot be adequately covered yet. Due to the openness (broadcast nature) of the wireless radio channel anyone can monitor or participate in the communication. Currently available security systems either do not meet all requirements or cannot be used in practice due to their high costs. Even key exchange procedures, which are an essential part of certain security systems, are still an unsatisfactorily solved problem [4]. Because of the known resource limitations in terms of computing power, battery power and memory of low cost sensors and other constraints presented in [5], WSN are a predestined target for attacks and common security mechanisms are difficult to implement. This is not only true from the protection point of view by, e.g. cryptographic algorithms, but also from a detection perspective by applying Intrusion Detection Systems (IDSs). IDSs are able to detect malicious behavior even when cryptography has been overcome. Furthermore, attacker abilities are increasing for instance by applying cloud/distributed computing or even quantum computation [7] allowing to immobilize or compromise WSN-nodes. The way IT-security is treated has to change into a sustainable prevention which transforms classical IT-security into sustainable cyber resilience.

In order to still preserve the requirement of low energy consumption in accordance with security, this work provides an overview on existing security mechanisms and proposes a future-proof security concept considering among others quantum-safe schemes. The remainder of this paper is structured as follows: Section II presents security goals in WSN as well as possible attack vectors. A literature review on security mechanisms including cryptographic mechanisms and intrusion detection techniques for WSN is provided in Section III. The proposed lightweight security concept including the novel Magic Number filter, to mitigate a specific DoS-attack is presented in Section IV. The evaluation in Section V deals with energy consumption measurements on WSN-ready CC1350 LaunchPad boards regarding the first two stages of the proposed concept. A short conclusion and a glance at the future work of the ongoing research work is finalizing the work in Section VI.

II. Security Goals & Attack Vectors

Compared to wired networks, WSN are more vulnerable to attacks due to the open communication in which an adversary can easily eavesdrop, intercept, inject and forge the communicated data. Utilizing cryptographic schemes such attacks can be mitigated in order to preserve the protection goals Confidentiality, Integrity, Authenticity, Non-repudiation, *Freshness* and *Availability*. The security primitives written in italics can not directly be achieved using cryptographic techniques. A detailed categorization of security attacks on WSN threatening the protection goals can be found in the work of [4]. According to [1], [5], [6], attacks targeted towards WSN can be categorized in each layer of the Open Systems Interconnection (OSI) model including e.g. Jamming attacks on the physical or network layer.

In the work of [8] it is stated that a DoS-attack or Service Degradation has the target of disabling a special host or server. This can be achieved by sending loads of unauthorized data at the same time. They can occur on several OSI layers for instance by involving malicious transmissions into the network e.g. injecting requests at a rate that overwhelms the nodes or by manipulating the routing information used for multi-hop data communication on the network layer. Such attackers can cause an abnormal energy consumption and thus decrease the lifespan of the sensor nodes. Because of the injection of false information a group of DoS are particularly devastating for resource-constrained battery-powered devices. A special type of DoS on the application layer is the sending of a large number of forged packets by an attacker to a sensor node with the intention that an applied Message Authentication Code (MAC) verification or decryption algorithm consumes a large amount of energy. With the multitude of packets sent, the battery is drained quite fast. This special DoS is hereinafter referred to as battery drain attack. To the best of the author's knowledge no existing work has targeted this kind of attack such that the proposed solution by applying Magic Numbers in a filtering stages is a novelty.

With the upcoming of first quantum computers, the era of the so-called *quantum nervousness* begins and represents a new type of threat not only for WSN. Quantum computers have a disruptive potential when it comes to weaken or even break all contemporary applied asymmetric cryptographic schemes such as RSA or Elliptic Curve Cryptography (ECC). Especially ECC is becoming increasingly widespread in IoT-environments due to the more efficient arithmetic, the low memory usage, shorter key sizes and lower CPU consumption compared to RSA or DSA [1]. Asymmetric cryptography with adequate key sizes [9] is considered very safe today, since the underlying mathematical problems such as efficient integer factorization or the calculation of the discrete logarithm are considered difficult even after years of investigation. However, already in 1994, Shor proposed an algorithm in [10] capable of breaking RSA and ECC in a reasonable amount of time if powerful quantum computers become reality. Symmetric cryptography, such as AES, is also affected by quantum algorithms. A practical attack by the so-called Grover algorithm [11] is in contrast far less fatal, since it is currently assumed that it can be compensated by doubling the key length. For cryptographic hash functions, quantum computers do not imply the doom of their security. The authors of [12] reckon that both SHA-256 and SHA3-256 need around 2166 logical qubit cycles to be cracked and if the quantum correction is handled by ASICs running at a few million hashes per second, Grover's algorithm would still need about 1032 years for cracking.

III. Security Mechanisms for WSN

Security mechanisms counteracting the above mentioned attacks while preserving the security goals for WSN are discussed in [8]. The basic defense mechanism in WSN is cryptography which directly protects the data. However, intrusion detection mechanisms complementary to cryptographic schemes are integral parts in holistic IT-security ecosystems.

A. Cryptographic Mechanisms

Nowadays, cryptography for secure communication is typically comprised of the following essential components: *key exchange* e.g. ECDH schemes; *public-key authentication* e.g. ECDSA signatures; *message encryption* e.g. AES-128; *message authentication* e.g. HMAC SHA-256. For each component various alternatives exist. However, with the threat of quantum computers, practical alternatives for e.g. public-key algorithms must be researched. Post-quantum cryptography (PQC) promises to remedy the situation when Shor's algorithm will be efficiently applicable on quantum computers since they can be carried out on non-quantum machines but promise to withstand the performance of quantum computers. Several quantum-safe alternatives to contemporary cryptographic schemes are presented in [13] including hash-based, code-based, lattice-based, multivariate-quadratic-equations and secret-key cryptography. Another type not mentioned in [13] is supersingular elliptic-curve isogeny cryptography. Even if this alternative is much closer to classical ECDH-schemes, it is very young and not well trusted [14]. Initial recommendations for post-quantum schemes, not intended for embedded domains, are provided by the PQCRYPTO project [15]. Some software implementations of lattice-based cryptography for low-cost microcontrollers targeted to IoT-applications are listed in [16]. A drawback is still the poor efficiency (in time and/or space) of most of the post-quantum schemes compared to contemporary cryptography which makes them hardly applicable on resource-constrained devices. The following sections deal with possible schemes targeted to WSN.

Key Exchange Mechanisms: According to [17], key management comprises the key deployment/pre-distribution, the key agreement as an authenticated key exchange, the member/node addition, the member/node eviction and the key revocation. Protocols for key management in WSN are presented in [5] and types for key agreements are discussed in [17]. Those comprise symmetric and asymmetric key agreements as well as ones over a trusted third party. Symmetric schemes demand less computing power but suffer from the issue of an initial key exchange over a secure channel compared to such based on asymmetric cryptography. Using symmetric keys among others is especially difficult when new nodes are brought dynamically into a network. The usage of symmetric keys installed on every node (pre-deployed) offers a great attack vector on which consecutive cryptographic schemes could depend on. For this reasons symmetric solutions are not recommended. A trusted third party for key agreement, e.g. Kerberos, is unattractive since large sensor networks are characterized with multi-hop communication and such solutions are not as energy-efficient as other methods for instance based on ECDH. Schemes based on asymmetric cryptography such as the work in [18] can be broken in the post-quantum age using Shor's algorithm. If the most prominent example NTRU could be used for a key exchange as proposed in [19] it would not be practically applicable in WSN since the 3-step handshake approach is associated not only with a large computational cost but also with a high communication overhead. Other key exchange mechanisms, BCNS15, Frodo, SIDH or McBits, implemented in the Open Quantum Safe project [20] aiming to integrate current post-quantum schemes are not optimized for the usage in WSN. With various generic and platform-specific optimization, a promising candidate for an IoT-enabled post-quantum key exchange is NewHope [16] which has been ported for the ARM Cortex-M architectures [21].

Signature/Verification Mechanisms: Signatures are necessary in order to authenticate for instance the key exchange process. Widely employed in the classical IT are the RSA or DSA signature mechanisms. Since often, signing and verifying in WSN is only used for the initial key exchange or the key renewal, the requirements in terms of memory or execution time are not as strong as with the continuously applied encryption/decryption functions. However, for resource constrained devices, limitations can be still cumbersome for the heavy computation involved schemes. ECDSA seems due to its efficiency a promising scheme to be applied in WSN. Examples are the lightweight mechanisms presented in [22], [23]. However, the mentioned approaches provide no protection when quantum computers become a considerable threat. Efficient post-quantum signature algorithms for constrained devices could help to remedy this situation. Some of the PQC schemes are Quasi-cyclic MDPC-based McEliece, HFEv-based Multivariate Signature Scheme, or Rainbow signature. Targeted to WSN, the work in [24] compares different post-quantum signature schemes on 128-bit security level. The most prominent ones are either based on lattices such as NTRUSign [25], BLISS [26] or are hash-based such as extended Merkle's signature scheme (XMSS) with similar approaches for IoT-environments [27] or ARMed SPHINCS [28]. The latter two are recommended by the PQCRYPTO project [15]. Especially ARMed SPHINCS based on SPHINCS-256 is a promising implementation for the embedded use. It is a high-security post-quantum stateless hash-based signature scheme and provides an effective replacement for signatures by combining XMSS, improved Winternitz One-Time Signature and Hash to Obtain Random Subset Trees few-time signature scheme in order to overcome the drawback of statefulness of XMSS. With the implementation on an ARM Cortex M3, the authors demonstrate that it is possible to generate and verify signatures on constrained devices.

Symmetric Encryption/Decryption Mechanisms: According to [29] the requirements of cipher schemes for WSN are energy consumption, program memory (storage), temporary memory (RAM) and execution time. Symmetric cipher schemes can be generally divided into block ciphers and stream ciphers. Exemplary schemes for block ciphers are AES, RC5, RC6, Skip Jack, HIGHT, BSPN and for stream ciphers RC4, Sosemanuk, HC-128, Dragon, LEX or Salsa/ChaCha [29], [30], [31]. The authors of [31] have implemented HC-128, LEX, Salsa20, Salsa20/12, Dragon in assembler and ported AES to a 8-bit AVR microcontroller. According to the authors, regarding encryption speed, all stream ciphers except for Salsa20 turned out to outperform AES. In terms of memory needs, Salsa20, Salsa20/12, and LEX are almost as compact as AES. For embedded applications with high throughput requirements, Sosemanuk is the most suitable cipher if its considerable higher memory needs can be tolerated [31]. The work in [30], in contrast, has compared different block and stream ciphers in software and suggests that a cryptographic scheme using AES achieves better performance for a wide range of channel qualities and provides significant improvement in energy efficiency compared to other schemes. The PQCRYPTO project recommends the AES-256 and Salsa20 with a 256-bit key [15]. Thus, the assembly supported AES from [32] seems a promising candidate for WSN-devices.

Message Authentication Mechanisms: In order to achieve message integrity and authentication, MACs are used, to recognize unauthorized and corrupted messages being transferred in a network. Those cryptographic constructions can either be defined over symmetric ciphers as modes of operation or, as the most common ones, can be based on one-way hash functions such as HMACs. Typically applied HMACs seem, due to the inherent energy limitations of WSN, not feasible. Possible message authentication codes for embedded devices are assembly-optimized HMAC implementations, the lightweight MAC Chaskey proposed in [33], the LMAC of [34], Poly1305 or the LightMAC [35] mechanism.

B. *Incident Detection Mechanisms*

Cryptographic mechanisms alone are not sufficient for a holistic security solution in WSN. IDS are a valuable supplement and a possibility to detect attacks by monitoring the events occurring in a computer system and/or network such that malicious actions attempting to compromise security primitives can be detected. A categorization of the main types including host-based and network-based IDS as well as their general detection methods (misuse-based and anomaly-based) can be found in [36], [37]. In recent years hybrid approaches have crystallized as the trend towards sophisticated intrusion detection solutions. Having more and more distributed connected devices, collaborative IDS promise to detect highly advanced attacks in the future. The application of classical IDS known from the office domain, e.g. Snort, Bro or Suricata, is due to the energy limitations not feasible in a WSN [4]. For this reason, intrusion detection has been classified as high-level mechanism which requires a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements [36]. A classification and overview of IDS including their distinctive features for WSN or recommendations for applications is presented in [36], [38].

IV. Lightweight WSN Security Concept

The proposed lightweight security concept is built around the filter-based processing stages shown in Fig. 1. Thus, in a resource preserving manner, incoming messages are running through stages characterized from low (stage 1) to high (stage 6) resource requirements in order to filter out inappropriate (malicious or corrupted) messages. Whereas stages 1-4 are recommended in order to provide sufficient protection of the communicated data, stages 5 and 6 can be seen optional depending on the available resources of a sensor node. An adversary who might be able to overcome one stage could be detected by the consecutive one. By choosing suitable lightweight schemes for stages 1-4, even highly resource constrained devices can be addressed.

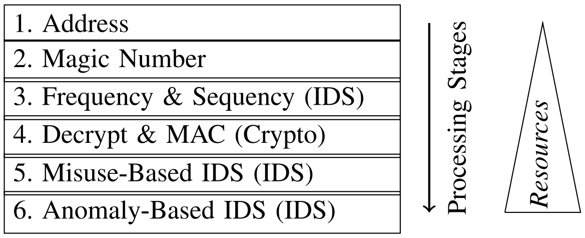
1. Address
2. Magic Number
3. Frequency & Sequency (IDS)
4. Decrypt & MAC (Crypto)
5. Misuse-Based IDS (IDS)
6. Anomaly-Based IDS (IDS)
Processing Stages
Resources

Fig. 1. Filter-based processing stages for incoming data

The Address stage filters messages that do not match the intended recipients address. A whitelist approach is suggested such that only messages with the defined destination addresses can be received and no additional energy is wasted if the message is not intended for the target node. Alternating codes or lightweight One-Time Passwords for each transmitted message are proposed as stage 2 in order to avoid for instance battery drain attacks. Thus, instead of first deciphering a message or verifying the MAC which can be quite resource consuming and depended on the message size, the Magic Number can be used to quickly check whether the message is valid. Both parties will generate the same sequence of Magic Numbers, based on the negotiated shared common secret obtained from stage 4, attach them to the message header and can then easily sort out forged messages a priori. After each key renewal the seed to generate the pseudo-random number sequence will be updated which in addition allows a re-synchronization if the pseudo-random number sequence drifted apart. This could happen for instance when an attacker was able to guess a correct number in one interval. Choosing the dimension for the Magic Numbers sufficient large will further reduce the attack surface. Since mechanisms such as the Keccak-based [39] Pseudo-Random Number Generator (PRNG) are quite resource-intensive, a more lightweight number sequence could be obtained by non-cryptographical but fast Xorshift-PRNGs proposed in [40]. Since the authenticity of messages is checked in stage 4, a non-cryptographically secure solution is sufficient for quickly sorting out inappropriate messages. An adversary who jams a message, steals the valid pseudo-random number and replays a forged message would be detected due to the delay in the next stage's Frequency filter. Stage 4 considers cryptographic schemes of the main building blocks stated in Section III with respective quantum-safe and lightweight candidates for the protection of communicating wireless sensor nodes. Additional encrypted or authenticated sequence or freshness values should be included within the payload of messages preventing for instance replay attacks. Wrongly decrypted messages or mismatches of MACs can be filtered in this stage especially if preceding stages failed.

The concept provides security features not only from a prevention but also a detection perspective. Lightweight and easy implementable IDS techniques are frequency and sequency methods for stage 3 known from instance of the CAN domain e.g. proposed in [41]. Thus, similar to the CAN-ID, each authenticated sensor node is sending messages either event- or period-triggered having a destination address in the frame structure. Based on the received messages, typical transmission intervals or sequences per destination address can be trained over a certain time period. The necessary calculations comprise only basic calculus and simple arrays/matrices to be stored which makes the algorithms perfectly applicable on WSN-devices. Applying for instance the frequency filter could help to mitigate further DoS-attacks on-the-fly. Similar to the Magic Number approach such a filter could abort the receive function and filter all consecutive messages if the interval expected does not match the trained interval. If in terms of available resources applicable, resource intensive misuse- and anomaly-based IDS are proposed for stage 5 and 6. As shown in the processing stages, the results from a misuse-based IDS of stage 5 are evaluated before passed to an anomaly-based IDS since founded on rules the former works significantly faster and is less computationally intense. The misuse-based IDS is therefore filtering a large number of malicious packets in advance and provides the basis for a downstream applied anomaly-based one in stage 6 (cf. [42]). Even if according to various literature they are not feasible in the WSN-field [4], the energy consumption can be decreased by the reduction of the detection frequency similar to [43]. Thus, the detection algorithm is applying sampling techniques known of classical IDS. In order to preserve energy consumption, a packet- and/or time-driven sampling mechanism as used in [44] is proposed.

V. Evaluation

The following evaluation scenarios are performed using LAUNCHXL-CC1350 LaunchPad boards equipped with a 32-bit ARM Cortex-M3 processor. Scope of the evaluation are measurements regarding the energy consumption of the processing stages 1 and 2 of Fig. 1 and discussions of the implication of a battery drain attack. A DC voltage source providing 3.3 V is used to source the board with an interconnected low-side shunt resistor (10 Ω). A LeCroy WaveRunner 610 Zi is used together with a Teledyne LeCroy PP008 passive probe to measure the voltage drop over the shunt in order to compute the energy consumption. The Code Composer Studio in Version 8.0.0.00016 has been used to program the boards via the onboard debugger. As basis projects, *rfEasyLinkEchoTx* and *rfEasyLinkEchoRx* are used from the Texas Instruments

Resource Explorer which demonstrate the usage of the EasyLink API. The board's idle current is approximately 7.6 mA.

The energy efficiency for secure data transmission does not only rely on the computational cost of the used cryptographic algorithms but also and mainly on the communication cost [45]. The influence on the energy consumption and therefore on the battery lifetime mainly for receiving messages in combination with their decryption or computation of MACs must therefore significantly be reduced. In order to demonstrate the impact of the Address filter in stage 1 of the proposed concept, the EasyLink_enableRxAddrFilter of the EasyLink library is evaluated. Fig. 2 shows the energy consumption of first the transmitting (TX) and afterwards the receiving (RX) signal with (upper plot) and without (lower plot) an applied address filter.

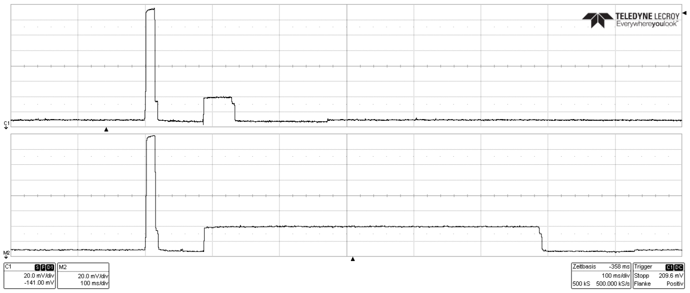

Fig. 2. Measurement of the TX/RX function with (upper plot) and without (lower plot) address filter

The average current amplitude for the transmission / reception of 74 bytes of data with an address filter is approximately 14 mA / 3 mA and the duration approximately 20 ms / 50 ms. The energy consumption yields approximately 924 μJ for transmission and 495 μJ for reception. The total board energy consumption yields 1.75 mJ / 1.43 mJ respectively. Without an receiving address filter, the reception function (duration of 500 ms) consumes approximately 4.95 mJ which yields a total board energy consumption of 17.49 mJ. This is more than a factor of ten that an applied address filter will save in terms of energy consumption per message. Nevertheless, an adversary is still able to send malicious messages with the correct address in order to exploit the resource consumption by message authentication verification or decryption mechanisms. The xoshiro128+ Xorshift number generator has been utilized to generate Magic Numbers to quickly check whether a message has been forged or not in a resource preserving manner in stage 2. The average current amplitude for generating a single number of the pseudo-random sequence is approximately 425 μA and the duration 3.76 μs. Thus, the energy consumption for the number generation is approximately 5.27 nJ and including the board consumption 99.57 nJ. In comparison with stage 4 to detect inappropriate messages, the energy consumption of the lightweight message authentication scheme LightMAC based on [35] and the symmetric cipher scheme aes-armcortexm from [32] have been measured. LightMAC would consume approximately 4.09 μJ and the AES implementation approximately 0.76 μJ both for the total board energy and 16 bytes of data. Even with the faster AES solution, the Magic Number approach is approximately seven times more efficient and, in addition, independent of the message size. An integrated Magic Number filter similar to the EasyLink_enableRxAddrFilter would abort the reception of a message if the Magic Number does not match. Thus, independent of the message size being transferred energy can be saved if the number of this simple check does not match.

VI. Conclusion & Future Work

In this work a future-proof lightweight security concept for WSN has been proposed suggesting a multi-staged filtering system including cryptographic and incident detection mechanisms. Security goals targeted to WSN are stated and attack vectors with a special focus on quantum threats as well as the DoS-specific battery drain attack are provided. A selection of essential building blocks for cryptographic schemes including key exchange, digital signatures, symmetric encryption and message authentication as well as intrusion detection mechanisms dedicated for WSN have been reviewed which found the basis for the proposed concept. The processing stages of the filtering system allows a resource-preserving processing of incoming packets such that e.g. malicious packets are filtered in a lightweight manner and even more advanced attacks can be detected or mitigated. Utilizing a Magic Number filter based on e.g. Xorshift functions allows to quickly sort out inappropriate battery drain attack messages. Further work will contain a more detailed characterization and specification of the Magic Number filter.

Special focus will be dedicated to integrate and compare the recommended cryptographic schemes and from the detection perspective to implement and assess the incident detection stages since they have been neglected in the current evaluation. Future work will comprise resource-preserving frequency- and sequency-techniques as well as more computationally complex misuse- and especially anomaly-based techniques stated in the literature review. In conjunction with an applied Address and integrated Magic Number stage, the holistic evaluation of the processing stages can be performed by embedding the concept in a WSN-framework such as [24].

Acknowledgment

This research work has been supported by the research projects no. 16KIS0539 of the German Federal Ministry of Education and Research and the Ministry of Education, Youth and Sports of the Czech Republic under grant no. LO1506.

References

[1] D. Mani and P. Nishamol, *A Comparison Between RSA and ECC in Wireless Sensor Networks*, International Journal of Engineering Research & Technology, Vol. 2, Issue 3, 2013

[2] R. Srinivasan, A. Sharmili, S. Saravanan and D. Jayaprakash, *Smart vehicles with everything*, 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016

[3] S. Popov, *The Tangle*, IOTA Whitepaper, [Online] https://iota.org/IOTA_Whitepaper.pdf, 2018

[4] N. Schmittberger, *Security in Event-Driven Wireless Sensor Networks* , PhD Thesis Freie Universität Berlin, [Online] http://page.mi.fu-berlin.de/eke/schmittb11security.pdf, 2010

[5] J. Sen, *Security in Wireless Sensor Networks*, CoRR, abs/1301.5065, [Online] http://arxiv.org/abs/1301.5065, 2013

[6] A. K. Sharma, S. K. Saroj and P. Kumar, *Distributed Intrusion Detection System for Wireless Sensor Networks*, IOSR Journal of Computer Engineering, Volume 14, Issue 1, pp. 61-70, 2013

[7] T. Vittor, T. Sukumara, S. Sudarsan and J. Starck, *Cyber security - security strategy for distribution management system and security architecture considerations*, 70th Annual Conference for Protective Relay Engineers (CPRE), 2017

[8] D. Costa, S. Figueredo and G. Oliveira, *Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions*, Cryptography, 1(1), 4, MDPI, 2017

[9] Bundesamt für Sicherheit in der Informationstechnik, *Cryptographic Mechanisms: Recommendations and Key Lengths*, BSI - Technical Guideline BSI TR-02102-1, [Online] https://www.bsi.bund.de/, accessed 03 July 2018

[10] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing, Volume 26 Issue 5, 1997

[11] L. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, p. 212, 1996

[12] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent and J. Schanck, *Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3*, Cryptology ePrint Archive, Report 2016/992, 2016

[13] D. Bernstein, J. Buchmann and E. Dahmen, *Post-quantum cryptography*, Springer, Berlin, ISBN 978-3-540-88701-0, 2009

[14] X. Bogomolec and J. Gerhard, *Post-Quantum Secure Cryptographic Algorithms*, CoRR, arXiv:1809.00371, [Online] https://arxiv.org/abs/1809.00371, 2018

[15] PQCRYPTO, *Initial recommendations of long-term secure post-quantum systems*, Horizon 2020 ICT-645622, [Online] http://pqcrypto.eu.org/docs/initial-recommendations.pdf, 2015

[16] R. Xu, C. Cheng, Y. Qin and T. Jiang, *Lighting the Way to a Smart World: Lattice-Based Cryptography for Internet of Things*, CoRR, abs/1805.04880, [Online] https://arxiv.org/abs/1805.04880, 2018

[17] U. Kumaran, M. Nallakaruppan and M. Kumar, *Review of Asymmetric Key Cryptography in Wireless Sensor Networks*, International Journal of Engineering and Technology, 2016

[18] K. Bindu, C. Aishani and M. Kamalakar, *A Secure Key Exchange Scheme in Wireless Sensor Networks Using Diffie Hellman*, Int. Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 9, 2016

[19] X. Lei and X. Liao, *NTRU-KE: A Lattice-based Public Key Exchange Protocol*, IACR Cryptology ePrint Archive, 718, 2013

[20] Open Quantum Safe Project, *Software for Prototyping Quantum-Resistant Cryptography*, [Online] https://openquantumsafe.org/, accessed 06 November 2018

[21] E. Alkim, P. Jakubeit and P. Schwabe, *A new hope on ARM Cortex-M*, IACR Cryptology ePrint Archive, [Online] https://eprint.iacr.org/2016/758.pdf, 2016

[22] M. Lavanya and V. Natarajan, *LWDSA: light-weight digital signature algorithm for wireless sensor networks*, Sadhana Vol. 42, No 10, pp. 1629-1643, 2017

[23] G. Ateniese, G. Bianchi, A. Capossele, C. Petrioli and D. Spenza, *Low-cost standard signatures for energy-harvesting wireless sensor networks*, ACM Transactions on Embedded Computing Systems (TECS), 16(3), 64, 2017

[24] C. Margi, R. Alves and J. Sepulveda, *Sensing as a Service: Secure Wireless Sensor Network Infrastructure Sharing for the Internet of Things*, Open Journal of Internet of Things, Volume 3, Issue 1, 2017

[25] B. Driessen, *Efficient Embedded Implementations of Security Solutions for ad-hoc Networks*, Diploma Thesis, Ruhr-University Bochum, [Online] https://www.emsec.rub.de/media/crypto/attachments/files/2010/04/da_driessen.pdf, 2007

[26] J. Howe, T. Pöppelmann, T. O'neill, M. O'sullivan and T. Güneysu, *Practical lattice-based digital signature schemes*, ACM Transactions on Embedded Computing Systems (TECS), 14(3), 41, 2015

[27] G. Pereira, C. Puodzius and P. Barreto, *Shorter hash-based signatures*, Journal of Systems and Software, Volume 116, Pages 95-100, 2016

[28] A. Hülsing, J. Rijneveld and P. Schwabe, *ARMed SPHINCS*, In Public-Key Cryptography, pp. 446-470, Springer Berlin Heidelberg, 2016

[29] A. Karuppiah and S. Rajaram, *Energy Efficient Encryption Algorithm for Wireless Sensor Network*, International Journal of Engineering & Technology (IJERT), Vol. 1, Issue 3, 2012

[30] X. Zhang, H. Heys and C. Li, *Energy efficiency of encryption schemes applied to wireless sensor networks*, Security and Communication Networks 5.7 (2012): 789-808, 2011

[31] G. Meiser, T. Eisenbarth, K. Lemke-Rust and C. Paar, *Efficient implementation of eSTREAM ciphers on 8-bit AVR microcontrollers*, International Symposium on Industrial Embedded Systems, 2008

[32] P. Schwabe and S. Ko, *All the AES you need on Cortex-M3 and M4*, International Conference on Selected Areas in Cryptography. Springer, Cham, 2016

[33] N. Mouha, B. Mennink, A. Herrewege, D. Watanabe, B. Preneel and I. Verbauwhede, *Chaskey : An Efficient MAC Algorithm for 32-bit Microcontrollers*, Selected Areas in Cryptography - SAC 2014, 2014

[34] A. Chowdhury and S. DasBit, *LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network*, 2015 IEEE Global Communications Conference (GLOBECOM), 2015

[35] A. Luykx, B. Preneel, E. Tischhauser and K. Yasuda, *A MAC Mode for Lightweight Block Ciphers*, Cryptology ePrint Archive, 2016/190, 2016

[36] I. Butun, S. Morgera and R. Sankar, *A Survey of Intrusion Detection Systems in Wireless Sensor Networks*, IEEE Communications Surveys & Tutorials, pp. 266-282, 2014

[37] M. Heigl, L. Doerr, A. Almaini, D. Fiala and M. Schramm, *Incident Reaction Based on Intrusion Detections Alert Analysis*, 2018 International Conference on Applied Electronics, Pilsen, pp. 1-6, 2018

[38] Y. Maleh, A. Ezzati, Y. Qasmaoui and M. Mbida, *A Global Hybrid Intrusion Detection System for Wireless Sensor Networks*, Procedia Computer Science, The 5th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2015), 2015

[39] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, S. Mangard and F. Standaert, *Sponge-Based Pseudo-Random Number Generators*, Cryptographic Hardware and Embedded Systems, Springer, 2010

[40] G. Marsaglia, *Xorshift RNGs*, Journal of Statistical Software, 8 (14), doi:10.18637/jss.v008.i14, 2003

[41] M. Marchetti and D. Stabili, *Anomaly detection of CAN bus messages through analysis of ID sequences*, 2017 IEEE Intelligent Vehicles Symposium (IV), Los Angeles, CA, 2017, pp. 1577-1583, doi: 10.1109/IVS.2017.7995934, 2017

[42] M. Weber, S. Klug, E. Sax and B. Zimmer, *Embedded Hybrid Anomaly Detection for Automotive CAN Communication*, Proceedings of the 9th European Congress on Embedded Real Time Software and Systems, Toulouse, France, hal-01716805, [Online] https://hal.archives-ouvertes.fr/ERTS2018/, 2018

[43] M. Riecker, *Lightweight Intrusion Detection in Wireless Sensor Networks*, Dissertation Technische Universität Darmstadt, [Online] http://tuprints.ulb.tu-darmstadt.de/4928/, 2015

[44] H. Taejin, K. Sunghwan, A. Namwon, N. Jargalsaikhan, J. Chiwook, K. JongWon and L. Hyuk, *Suspicious traffic sampling for intrusion detection in software-defined networks*, Journal Computer Networks, 2016

[45] G. Bianchi, A. Capossele, A. Mei and C. Petrioli, *Flexible key exchange negotiation for wireless sensor networks*, Proceedings of the fifth ACM international workshop on Wireless network testbeds, experimental evaluation and characterization, pp. 55-62, 2010