Paper

# A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks

Krzysztof Daniluk[a] and Ewa Niewiadomska-Szynkiewicz[a,b]

[a] *Institute of Control and Computation Engineering, Warsaw University of Technology, Warsaw, Poland*
[b] *Research and Academic Computer Network (NASK), Warsaw, Poland*

**Abstract—Data security and energy aware communication are key aspects in design of modern ad hoc networks. In this paper we investigate issues associated with the development of secure IEEE 802.15.4 based wireless sensor networks (WSNs) – a special type of ad hoc networks. We focus on energy aware security architectures and protocols for use in WSNs. To give the motivation behind energy efficient secure networks, first, the security requirements of wireless sensor networks are presented and the relationships between network security and network lifetime limited by often insufficient resources of network nodes are explained. Second, a short literature survey of energy aware security solutions for use in WSNs is presented.**

***Keywords—energy aware security architectures, routing protocols, security protocols, wireless sensor networks, WSN.***

## 1. Introduction

A Wireless Sensor Network (WSN) is a distributed system composed of hundreds or thousands small-size, inexpensive, embedded devices deployed densely over a significant, often hostile area [1]. Each device can run applications and participate in transferring data to recipients within its range. The lack of fixed network infrastructure components in WSN allows creating unique topologies and enables the dynamic adjustment of individual nodes to the current network structure in order to execute assigned tasks.

WSNs have been identified as one of the most important technologies of this century. Due to their sensing capabilities, CPU power and radio transceiver plenty of sensor devices can be deployed in a sensing area, hence they can be used in applications, in which traditional networks are inadequate. However, nodes comprised by the network are often small battery-fed devices, which means their power source is limited [1]–[3]. The network's throughput is also limited. Moreover, the quality of wireless transmission depends on numerous external factors, like weather conditions or landform features. Part of those factors change with time.

Conventional networks with fixed infrastructure require protection against injection or modification of disseminated data packets and eavesdropping. Most applications of WSNs require the same protection. All well known attacks including traffic analysis, node replication, Denial of Service (DOS) and physical manipulating should be concerned. The security threads and attacks for all layers of the OSI model are discussed in [4]. Moreover, due to the spontaneous nature and shared wireless medium, sensor networks are more vulnerable to security attacks than wired ones. Using a computer with a wireless network adapter, anyone can gain an access to an unprotected network. Hence, the outsider can monitor the network, participate in the communication and easily launch attacks.

The main contribution of this paper is to point out the problems concerned with energy aware security architectures and protocols for IEEE 802.15.4 based WSN. It is a topic that has been a subject of intensive research in the recent years. The question is how to ensure the expected security level taking into account scarce resources of devices (network nodes). In Sections 2 and 3, we briefly summarize security requirements and security issues in WSN. Next, we present energy aware security architectures and protocols (Section 4), and energy efficient secure routing protocols (Section 5). The paper concludes in Section 6.

## 2. Security Requirements of WSN

Security for wireless sensor networks should focus on the protection of the data itself and the network connections between the nodes [5]–[8]. In general, security requirements often vary with application. In WSNs we can distinguish the following important requirements of security capabilities: authentication and authorization, availability, confidentiality, integrity and freshness. Thus, we need some mechanism for access authorization and protecting a mobile code. In many applications we need to protect fair access to communication channels and at the same time we often need to hide the information about physical location of our sensor node. Moreover, we need to secure routing and we have to defend our network against denial of service, malicious flows, node capturing and node injection, etc.

**Authorization**. Data authorization specifies access rights to resources and is strongly related to access control. Access control should prevent unauthorized users from participating in network resources. Hence, only authorized

users can join a given network. Access control relies on access policies that are formalized, like access control rules in a computer system. Most modern operating systems include access control.

**Authentication**. Message authentication implies a sender verification using cryptographic key. Authentication mechanisms are used to detect maliciously or spoofed packets. They are especially important in WSNs which use a shared wireless medium. In case of unicast transmission, an authentication can be guaranteed by symmetric key cryptography, using Message Authentication Code (MAC) in IEEE 802.15.4. Broadcast authentication requires more complex solutions (see [9]).

**Availability**. In secure network data should be safe and accessible at all times. Availability guarantees the survivability of network services against Denial-of-Service (DoS) attacks that can be launched at any layer of a wireless sensor network, and may disable a given device (network node) permanently. Moreover, DoS attack involved excessive computation and communication may exhaust battery charge of a sensor device.

**Confidentiality**. In WSN keeping sensitive data secret is the most important issue in case of critical applications in which highly sensitive data (secret keys, sensitive measurements, etc.) are collected and transmitted. Data confidentiality ensures that sensitive data is never disclosed to unauthorized users or entities. Hence, measurement data should not be available to neighboring nodes, and secure channels between nodes should be created. To protect a network against cyberattacks and malicious nodes, the routing information and sensor identities should remain confidential too. The standard approach to prevent end-to-end data confidentiality is to encrypt the data with a secret key.

**Integrity and freshness**. Data integrity is the quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data. It is achieved by preventing unauthorized insertion, modification or destruction of data. In WSNs a malicious node may change messages to perturb the network functionality. Moreover, due to unreliable communication channels it is easy to inject infected packets or alerted data. In WSNs data integrity guarantees that a message being transferred is never corrupted, but providing data integrity is not enough for wireless communication. The compromised sensor nodes can listen to transmitted messages and replay attacks. Data freshness protects data against replay attacks by ensuring that the transmitted data is recent one.

## 3. Security in WSN

Cryptography is the common approach for defense against cyber attacks. However, maintaining an appropriate level of security and protection of sensitive information transmitted by a wireless sensor network requires solving many issues that are not present in traditional computer networks, and it is a challenging task [8], [10]. It should be underlined that the primary objective of wireless sensor networks is to make measurements for as long as possible. To do this it is essential to minimize energy use by reducing the amount of inter-node transmission and using energy aware algorithms and protocols [1], [2]. Due to limited resources of nodes forming WSN a balance between security capability and lifetime performance has to be obtained. Strong security protocols based on an asymmetric cryptography are difficult to implement. In general, asymmetric signatures are long and need high communication overhead, thus they are impractical for WSN applications. On the other side, week security protocols based on a symmetric cryptography may be easily broken. Moreover, due to a hostile deployment area, it is difficult to perform continuous surveillance of a network. To design a completely secure sensor network, security must be integrated into each node of WSN. Any network node implemented without any security could easily become a point of attack. Therefore, it is crucial to design WSN with security in mind from the very beginning. It is obvious that security usually adds some communication overhead and requires intensive computation and memory that is concerned with increased power consumption. The integration of security techniques in processing and communications simply allows for more efficient use of limited resources.

In general, three types of key management security schemes can be considered:

- *Trusted server scheme*. The symmetric key cryptography for data encryption is used. The process of establishing the key agreement between two communicating nodes is executed in the base station. Each node has to store only a single secret key. Thus, this solution is memory efficient, but energy expensive due to transmission overhead – each node has to communicate with the base station many times.
- *Self enforcing scheme*. The public key cryptography for communication between sensor nodes is used – DSA or RSA cryptography schemes. The disadvantage is that both DSA and RSA require complex computations (computing and energy expensive solution).
- *Key-predistribution scheme*. The symmetric key cryptography with limited number of keys stored in each sensor node is proposed. This solution is energy efficient – it does not introduce any additional transmission overhead for key exchange.

In many secure architectures and routing protocols, the clustering schemes for grouping all network nodes into disjoint and mostly non-overlapping clusters are applied to WSN [11], [12]. Generally, a cluster formation in WSN is based on the following characteristics: every node has to be connected to some clusters, nodes in a cluster must be able to communicate with others, often maximum diameter of all clusters in the network is the same. Most algorithms form clusters in distributed way through local broadcasts

with a maximum one or several (not many) hops. The cluster size is adapted to network capabilities and objectives. The cluster head is usually pre-assigned or picked randomly from the deployed set of nodes. Finally, we obtain a hierarchical communication structure: base station, cluster heads (various levels) and the lowest level formed by members of clusters (remaining nodes).

# 4. Energy Efficient Security Architectures and Protocols

In this section, we survey some of more and less common security solutions for IEEE 802.15.4 based networks. We start from the short description of the IEEE 802.15.4 security implementation. Next, we present various energy efficient architectures that can be employed in physical, data link, network, and middleware layers of the OSI communication model.

## *4.1. Security in IEEE 802.15.4*

IEEE 802.15.4 is one of the first standards defining the radio and the medium access control layer for a low-power wireless sensor networks. ZigBee [13] is an industry alliance working on the 802.15.4 and upper protocol layers. Medium Access Control (MAC) protocols guarantee efficient access to the communication media while carefully managing the energy allotted to the node. This goal is typically achieved by switching the radio to a low-power mode based on the current transmission schedule. The comprehensive summary of MAC protocols for WSNs, and results of simulations that show their capabilities and efficiency in terms of the energy consumption are presented in [14]. The IEEE 802.15.4 network standard specification provides several security suits [15], [16]. The security suite specification defines the algorithms and operations that will be performed depending upon the security services to be provided. Each node can operate in secured or unsecured mode. A globally shared secret cryptographic key to message encryption and authentication is implemented. Eight security suites are defined in the IEEE 802.15.4 standard, and presented in Table 1. Each suit means a kind of cryptographic algorithm, the mode of block cipher, message authentication code, and the size of message authentication code. We can classify these suits based on provided properties, i.e., no security, encryption only (AES-CTR), authentication only (AES-CBC-MAC), and both encryption and authentication (AES-CCM). Thus, confidentiality is achieved through Advanced Encryption Algorithm (AES) in Counter mode (CTR), integrity through AES in Cipher Block Chaining Message Authentication Code (CBC-MAC) mode. The combination is offered with AES in the CTR with CBC-MAC mode (CCM).

Table 1
IEEE 802.15.4 security suite

| | Security suite | Description |
|---|---|---|
| #0 | Null | No security (default) |
| #1 | AES-CTR | Encryption only, CTR mode |
| #2 | AES-CBC-MAC-32 | 32 bit MAC |
| #3 | AES-CBC-MAC-64 | 64 bit MAC |
| #4 | AES-CBC-MAC-128 | 128 bit MAC |
| #5 | AES-CCM-32 | Encryption and 32 bit MAC |
| #6 | AES-CCM-64 | Encryption and 64 bit MAC |
| #7 | AES-CCM-128 | Encryption and 128 bit MAC |

## *4.2. SPINS: Security Protocol for Sensor Network*

The SPINS protocol developed by A. Perrig *et al.*, is described in [17]. It consists of two secure building blocks, i.e., Secure Network Encryption Protocol (SNEP) and micro version of Timed Efficient Stream Loss-tolerant Authentication ($\mu$TESLA). SNEP is used to provide confidentiality using encryption, and authentication, integrity and freshness of data using Message Authentication Code (MAC). In this approach all cryptographic primitives are constructed from a single block cipher for code reuse. Thus, the communication overhead is limited.
$\mu$TESLA is used for broadcasted data authentication. $\mu$TESLA requires that the base station and network nodes are loosely time-synchronized, and each node knows an upper bound on the maximum synchronization error. It generates authenticated broadcast message using symmetric key, and introduces asymmetric cryptography by delaying the disclosure of the symmetric keys. Therefore, $\mu$TESLA provides stronger security for networks with constrained resources. The implementation of SPINS requires about 220 bytes of RAM and 1580 to 2674 bytes of program space. An increase of energy consumption for security is about 20%.

## *4.3. TinySec: Link Layer Security Architecture for Wireless Sensor Networks*

The problem with SPINS is that it has not been yet fully specified and implemented. TinySec is a link layer security architecture designed by Ch. Karlof *et al.*, and presented in [18]. Similarly to the SNEP protocol, it provides authentication, message integrity and confidentiality services. Replay protection has been intentionally omitted – the authors argued that this service belongs to the higher layers of the OSI model. The message authentication and integrity is provided using MAC, message confidentiality using encryption. Two security modes are possible – authentication only and authenticated encryption. In case of the first mode, the entire packet is authenticated using MAC, but the payload data is not encrypted. In case of the second mode, the payload data is encrypted and then authenticated with a MAC. Any keying mechanisms can be employed (single network-wide keys, per-link keys, group keys, etc.). TinySec is designed as a lightweight, energy efficient security package. It can be easily integrated into any WSN application. The implementation of TinySec requires about

728 bytes of RAM and 7146 bytes of program space. An increase of energy consumption depends on the mode and network technology, and is about 3% to 9,1% higher in compare to a normal TinyOS packet transmission.

### *4.4. LLSP: The Link-Layer Protocol*

A Link-Layer Protocol (LLSP) was designed by L. E. Lighfoot *et. al*., and is described in [19]. The aim was to develop a protocol with less energy requirements than TinySec. LLSP guarantees various security requirements but focuses on three security services: message authentication, message confidentiality, and replay protection. AES-CBC mode of operation as the data encryption scheme is implemented in LLSP. The unique design of AES-CBC provides semantic security, i.e., encrypting the same plaintext twice will produce two different ciphertexts. A synchronous 4-byte counter between the sender and receiver pair is proposed to replay protection. Feedback Shift Register (FSR) is used to update this counter. The LLSP packet format is based on the TinySEC one (see Fig. 1). The difference is in a size – two byte counter values (Ctr) are removed from the security overhead in LLSP. As it was mentioned above both sender and receiver maintain a synchronous counter. Hence, the counter value has not to be transmitted, so the counter bytes are eliminated from each message packet. Thus, the LLSP security protocol reduces the energy usage without decreasing the security level.

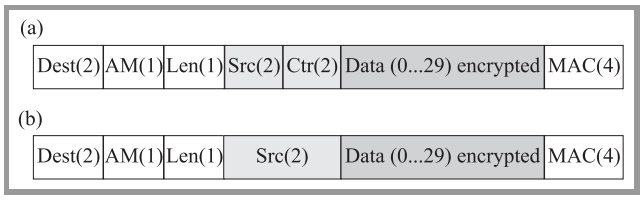


***Fig. 1.*** Packet format in TinySec (a) and in LLSP (b).

The LLSP secure protocol was evaluated via simulation and compared with the TinySec protocol. Both applications were executed in the TOSSIM simulator (docs.tinyos.net/index.php/TOSSIM). The results are presented in [19]. From these results we can see that similar to most security protocols, the computational and energy costs increase for each packet transmission. It is concerned with extra computations and the larger packet size due to the security overhead. However, the authors of the LLSP protocol claim that using their solution the energy consumption is about 15% smaller than for TinySec, and latency reduction is about 3%.

### *4.5. LEAP/LEAP+: Localized Encryption and Authentication Protocol*

LEAP [20] and LEAP+ [21] are lightweight, energy efficient security protocols for large scale sensor networks. They provide confidentiality and authentication services. LEAP was designed as a key management protocol to provide secure communication in WSNs. Due to various security requirements for different types of messages four types of keys for each network node are established: an individual key shared with a base station, a pairwise key shared with another node, a cluster key shared with a group of neighboring nodes, and a group key globally shared with all nodes in a network. The implementation of LEAP requires about 17.8 KB of program space. The RAM usage and energy costs depend on the number of nodes in a network.

### *4.6. Security Protocol Based on NOVSF*

The cluster-based security protocol proposed in [22] uses a symmetric cryptography algorithm to guarantee security. To reduce the drawbacks of a symmetric cryptography and provide complete security, it employs the code-hopping technique using the Non-Orthogonal Variable Spreading Factor (NOVSF) codes. The NOVSF is an implementation of the non-blocking transmission of CDMA. In NOVSF codes, each OVSF code has 64 time slots, and any number of these time slots can be assigned to a channel. In NOVSF, the data blocks are assigned to time slots using different permutations in every session, Fig. 2. Hence, the blocks

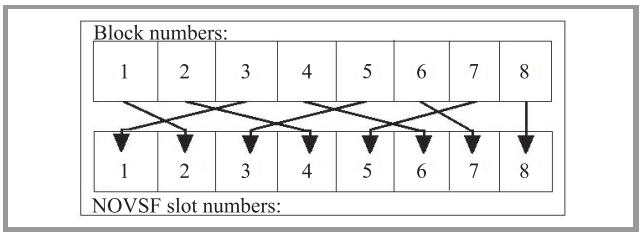


***Fig. 2.*** Code-hopping technique.

of data are finally mixed, and such reordering method supports security. The algorithm operates as follows. First, it is assumed that all network nodes are grouped into disjoint and mostly non-overlapping clusters. As a result, a hierarchical communication structure consisting of a base station, cluster heads and the lowest level formed by members of clusters is obtained. Secondly, the following steps of the algorithm are performed:

*Step 1*: A base station periodically broadcasts the session key.

*Step 2*: Sensor nodes generate their cryptographic keys.

*Step 3*: The encrypted data are transmitted from sensor nodes to cluster heads using NOVSF code-hopping technique.

*Step 4*: Each cluster head appends its identifier number (ID) to this data and then forwards such data to the higher level cluster heads.

*Step 5*: The message is decrypted and authenticated by the base station.

To sum up, the transmission between nodes and cluster heads is encrypted. Based on periodically changed user specific session keys and NOVSF codes assigned to each node the authentication of messages is performed. Moreover, changing encryption keys from time to time guarantees data freshness in a network. The CBC-MAC protocol is used to provide data integrity. The total memory space for applied cryptographic primitives are about 2 KB. Hence, applying the NOVSF code-hopping technique increases security capabilities without requiring additional energy.

### *4.7. LSec: Lightweight Security Protocol*

The Lightweight Security Protocol for distributed wireless sensor network (LSec) is described in [23]. It is the energy and memory efficient technique that assumes grouping network nodes into clusters. LSec provides following security capabilities: authentication, authorization, confidentiality of data, and protection against intrusions and anomalies. Both symmetric and asymmetric security schemes are used.

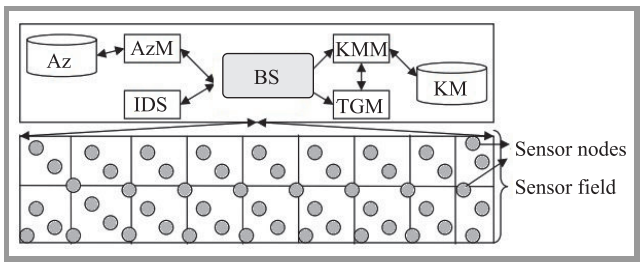


***Fig. 3.*** LSec system architecture.

The LSec architecture consists of the following modules (see Fig. 3):

- KMM key management module: stores public and shared secret key of each node with a base station (BS) to the database (KM),
- TGM token generator module: generates the tokens for the requesters,
- AzM authorization module: checks whether a particular node is allowed to communicate with other node or a group of nodes,
- IDS intrusion detection; cluster heads send alert messages to IDS (lightweight mobile agents are installed in cluster heads).

LSec combines the features of trusted server scheme and self enforcing security scheme described in Section 3. It is assumed that the base station is the trusted party that never is compromised. Only the base station has an access to the public keys of all nodes in the network, and communicating nodes know each other's public keys only during the time of connection establishment. For every session, new random secret key is used. Each node has to store six keys (public key of node, private key of node, public key of BS, group key, public key of other node, session key). 72 bytes of memory are needed to store these keys. An asymmetric scheme is used for sharing ephemeral secret key between communicating nodes. Data is encrypted by using symmetric schemes. LSec is employed in the middleware layer of the communication model. It is scalable and memory efficient solution.
Authors claim that LSec is highly scalable and memory efficient – it introduces only 74.125 bytes of transmission and reception cost per connection. It provides stronger security and has the advantage of simple secure defense mechanism against compromised nodes.

### *4.8. HASF: The Hybrid Adaptive Security Framework*

Hybrid Adaptive Security Framework (HASF) is a security architecture developed by T. Shon *et al.*, and described in [24]. This framework provides security capabilities with less extra energy usage than TinySec. In HASF, security functions are embedded to the network layer and the link layer (MAC) of the OSI model separately. The main idea is to provide hybrid adaptive security suite to each packet transmitted in a given WSN. The Hybrid Adaptive Security Suite (HASS) proposed in HASF is almost the same as the security suite proposed for IEEE 802.15.4, and presented in Table 1. The difference to commonly used architectures in HASS are as follows:

- *null* security is not provided,
- security suite is dynamically applied to MAC frame due to a type of a given WSN.

Three network characteristics are distinguished: *public*, *commercial*, *private*. Various security capabilities are provided to these groups of network. None confidentiality is guaranteed for public networks, more security capabilities are provided in commercial networks, and the strongest security is provided in private networks. All data are divided into control and application. *Control data* means a message or signal to manage the network operation. *Application data* means a kind of data concerned with WSN services. The attributes of these data are: periodic, urgent-periodic, on-demand, event-driven. The decisions on security levels in case of different network characteristics are presented in Table 2. In [24] authors discuss the results of application of their framework to a testbed network formed by the devices using HASS approach. They compared three kinds of nodes: IEEE 802.15.4 based system with no security, HASS based system with the AES encryption algorithm,

Table 2
Hybrid Adaptive Security Suite decision table

| Feature | | #1 | #2 | #3 | #4 | #5 | #6 | #7 |
|---|---|---|---|---|---|---|---|---|
| Public (32) | App | + | + | | | | | |
| | Ctrl | + | | | | + | | |
| Commercial (64) | App | | | + | | + | | |
| | Ctrl | + | | | | | + | |
| Private (128) | App | | | | + | | + | |
| | Ctrl | + | | | | + | | + |

Table 3
Summary of selected security architectures for WSN

| Architecture | Security services | Properties |
|---|---|---|
| SPINS | Authentication, authenticated broadcast, confidentiality, integrity, freshness. | Consists of SNEP and $\mu$Tesla (secure building blocks). Symmetric cryptography support. Encryption (CTR mode), Block Cipher (RC5). Not fully implemented and specified. Requires 2674 bytes of program space (max). Transmission overhead to 20%. |
| TinySec | Authentication, confidentiality, integrity, replay protection. | Link layer architecture easily integrated into WSN. Symmetric cryptography support. Encryption (CBC mode), Block Cipher (Skipjack). Requires 728 bytes of RAM, 7146 bytes of program space (max). Transmission overhead to 9.1%. |
| LLSP | Authentication, confidentiality, replay protection. | Link layer architecture. Symmetric cryptography support. Semantic security. 2 bytes less packet format (energy cost reduction without security decreasing). Transmission overhead to 7.7%. |
| LEAP/LEAP+ | Authentication, confidentiality, intrusions protection, anomalies protection. | Symmetric cryptography support. Encryption (RC5), Block Cipher (RC5). Four types of keys available for each sensor node: individual, pairwise, cluster, group. Defence against: HELLO Flood, Sybil, Wormhole attacks. Requires about 17.8 KB of program space. RAM usage and transmission overhead depend on the number of nodes. |
| NOVSF-based | Authentication, confidentiality. integrity, freshness. | Works partially in the physical layer. Symmetric cryptography support. The security increased via code-hoping technique using NOVSF data blocks (assigned to time slots using permutations in every session). User specific session keys (periodically changed). Clustering-based algorithm. Requires about 2 KB of memory space. |
| LSec | Authentication, authorization, confidentiality, replay protection, intrusions protection, anomalies protection. | Both symmetric and asymmetric cryptography support. Public Key cryptography support. Base station – the trusted party – a single point of failure. Implemented in the middleware. Clustering-based algorithm. Simple Secure key exchange scheme: 6 keys that takes only 72 bytes of memory. Transmission overhead to 8.33%. |
| HASF | Authentication, confidentiality, integrity. | Provides Hybrid Adaptive Security Suite. Security functions embedded to network and link layer separately. Security mechanism dynamically applied to MAC frame. Three network types with different security (public, commercial, private). Transmission overhead to 4.8%. |

and the Crossbow device based on TinySec architecture and the RC5 encryption algorithm. In the case of described experiments, the extra energy usage due to providing security functionalities was about 4.8% in case of HASS based system and 5.2% in case of TinySec based Crossbow system. The results confirmed that HASF outperforms the other common security techniques.

### *4.9. Summary of Security Architectures*

The Table 3 presents the summary of our survey – security architectures, provided services and their main properties.

## 5. Secure Energy Efficient Routing Protocols

Security architectures using a globally shared key are ineffective in presence of insider attacks or compromised nodes. Therefore, more sophisticated defense mechanisms are necessary to provide reasonable protection against wormholes and insider attacks, and detect malicious nodes. Secure routing protocols can be used to improve WSN security. In this section, selected routing protocols for secure networks are presented. Similarly to the solutions described in previous sections we focus on energy aware solutions.

### *5.1. SERP: Secure Energy Efficient Routing Protocol*

The secure energy efficient routing protocol for wireless sensor networks (SERP) is described in [25]. The main idea of this protocol is to provide a robust transmission of authenticated and confidential data from the source sensor with limited energy budget to the base station. It is dedicated to WSNs with densely deployed relatively static sensor devices.

Three main objectives were considered during design of SERP:

– energy aware organization of the network to ensure energy efficient transmission, and finally maximum lifetime of the network,

– secure transmission; nodes should have the capability to detect falsely injected reports,

– robust and resilient transmission; any node failure would not greatly hamper the performance of a network.

The protocol operates in two main phases: creating a backbone network and secure data transmission. A sink rooted tree structure is created as the backbone of the network taking into consideration balanced energy consumption. Next, a minimum number of forwarding nodes in the network is selected. The backbone network is restructured periodically. It is used for authenticated and encrypted data delivery from the source sensors to the base station. A one way hash chain and pre-stored shared secret keys are used for ensuring secure data transmission. An optional key refreshment mechanism that could be applied depending on the application is introduced for data freshness.
The energy saving mechanism is based on disable the radio transceivers of selected nodes. The nodes in a network can operate in two main states: *non-forwarding* – the transceiver is switched off, *forwarding* – both transceiver and sensing devices are switched on. It is assumed that after the backbone structure is constructed, all nodes are either in forwarding or non-forwarding states. Nodes with the non-forwarding state turn off their radio transceivers while keeping the sensing device active. On the other hand, forwarding nodes keep both radio and sensing device active. All nodes sense the environment, and after detecting any event the non-forwarding nodes turn on their radios and transmit data towards the base station via nodes in a selected path.
The SERP protocol was evaluated via simulation. Ns-2 simulator (www.isi.edu/nsnam/ns/) was used for performance analysis. SERP was compared with two popular energy aware routing protocols – LEACH [26] and EAD [27]. The simulation results are presented and discussed in [25]. The authors claim that SERP is a very competitive solution compared to the LEACH and EAD protocols w.r.t. energy requirements. Moreover, SERP provides security functionalities.

### *5.2. EENC: Energy Efficiency Routing with Node Compromised Resistance*

A novel energy efficiency routing protocol with node compromised resistance (EENC) was developed by K. Lin *et al.*, and described in [28]. EENC bypasses the compromised nodes and improves the accuracy of packets under the condition of balancing the energy consumption. The reinforcement learning based on the ant colony optimization is used to complete routing tables. The trust values are assigned to all nodes of a network. The trust value is computed and based on the multiple behavior attributes such as: packet drop rate, forwarding delay rate, etc. These values are used to detect the malicious nodes. Each node in a WSN computes the trust values of its one hop neighbors. The idea of EENC was to provide security with minimal energy consumption. To achieve this, each node storages trust values of all its neighbors and manages its energy resources.
The EENC protocol operates as follows. To transmit data the secure and energy efficient route is computed. The calculation process consists of many rounds, each divided into three phases.

- Routing detecting phase. A certain number of forward ants are generated to search for route leading to the sink. Each ant records the information about the minimum amount of energy and minimum trust value for nodes along the path, and the hop number for each node.

- Pheromone updating phase. The sink node generates a backward ant, which carries all data collected by the forward ant. These data are used to update the pheromone value concerned with each node in a path.

- Routing maintaining phase. The route for a given source and sink nodes is established based on trust values and updated pheromone values of the nodes carried during the pheromone updating phase.

The EENC protocol was evaluated via simulation. The considered performance metric included lifetime of a network and a packet correctly received ratio. The EENC performance was compared with two other routing algorithms, i.e., DRP and MTRP described in [29]. Simulation results presented in [28] confirm that the routing established via EENC can bypass most compromised nodes in the transmission path and EENC has high performance in energy efficiency. It was observed in the experiments that the calculated lifetime and the successful packet delivery ratio were much higher for EENC than those obtained for DRP and MTRP.

### *5.3. REWARD Routing Protocol*

The REceive WAtch ReDirect (REWARD) routing protocol for WSNs is described in [30]. This algorithm can be used to detect black hole attacks [4]. In such attacks, a malicious node acts as a black hole to attract all the traffic in a WSN through a compromised node. A compromised node is usually placed in the center and looks attractive to surrounding nodes and collect most traffic destined for a base station.
In REWARD, the distributed database including suspicious nodes and areas is created. Two types of broadcast messages, i.e., MISS (Material for Intersection of Suspicious Sets) and SAMBA (Suspicious Area, Mark a Black-hole

Attack) are used to organize this database. MISS is used to detect identifiers of malicious nodes, and SAMBA is used to identify physical locations of suspicious nodes.
The operation of the REWARD protocol is as follows. In case of demand-driven routing protocols, the query for path establishing is sent to the destination node. The destination node sends its location and waits for a packet. The destination node broadcasts a MISS message if a packet does not arrive within a specified period of time. It copies the list of all the involved nodes from the query to this MISS message – these nodes are under suspicion. The ratings for the nodes are introduced, and path metrics are calculated by averaging the node ratings in the path. The path with the highest value of a metric is selected – in this way the suspicious nodes are avoided. If a node attempts a black hole attack and drops a package, it is detected by the next node in the path. After a predefined time period, the node transmits the packet changing the path and broadcasts a SAMBA message that provides the location of the black-hole attack.
REWARD is the energy aware protocol and can be applied to networks formed by devices that can tune their transmit power. Different levels of security with less and more overhead according to a network capabilities are provided. The performance of the protocol is discussed in [30]. The authors compared the energy overhead of two variants of REWARD.

## 6. Summary and Conclusions

Many challenges arise from application of wireless ad hoc networking. We focused on one of them that is very important in wireless sensor networks – secure data protection and data transmission in WSN with limited resources. The paper provides a short overview of some representative energy efficient security techniques. We briefly discussed the security requirements of WSNs and showed the relationships between techniques for forming secure networks, and energy aware WSNs. Next, we described and compared based on literature survey selected energy aware architectures and protocols in WSNs that can be implemented in the physical, data link, network, and middleware layers of the OSI model.
In summary, we can say that due to scarce resources, unique properties of wireless sensor networks, and often hostile environments it is a challenging task to protect sensitive information transmitted by nodes forming a WSN. Due to limited resources of nodes that form WSN many solutions providing strong security are impractical in this type of network. Therefore, we can find many security considerations that should be investigated in the nearest future.

## Acknowledgment

This work was partially supported by National Science Centre grant NN514 672940.

## References

[1] M. C. Vuran, I. F. Akylidiz, *Wireless Sensor Networks*. Wiley, 2010.

[2] E. Niewiadomska-Szynkiewicz, P. Kwaśniewski, and I. Windyga, "Comparative study of wireless sensor networks energy-efficient topologies and power save protocols", *J. Telecom. Inform. Technol.*, no. 3, pp. 68–75, 2009.

[3] A. Tiwari, P. Ballal, and F. L. Lewis, *Energy-efficient wireless sensor network design and implementation for condition-based maintenance*, *ACM Trans. Sensor Netww (TOSN)*, vol. 3, no. 1, pp. 1–23, 2007.

[4] K. Sharma, M. K. Ghose, D. Kumar, "A comparative study of various security approaches used in wireless sensor networks", *Int. J. Adv. Sci. Technol.*, vol. 17, pp. 31–44, 2010.

[5] M. Ahmad, M. Habib, and J. Muhammad, "Analysis of security protocols for Wireless Sensor Networks", in *Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD 2011*, Shanghai, China, 2011, vol. 2, pp. 383–387.

[6] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks", *J. ACM Trans. Sensor Netw. (TOSN)*, vol. 5, no. 3, 2009.

[7] S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, S., *Energy efficient schemes for wireless sensor networks with multiple mobile base stations*, in *Proc. IEEE Global Telecom. Conf. GLOBECOM'03*, San Francisco, USA, 2003, vol. 1, pp. 377–381.

[8] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: a survay, in *Security in Distributed Grid, Mobile and Pervasive Computing*, Y. Xiao, Ed. Auerbach Publication, 2007.

[9] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. Fun Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards", *Comp. Commun*., vol. 30, no. 7, pp. 1655–1695, 2007.

[10] H. Kumar and A. Kar, "Wireless sensor network security analysis", *Int. J. Next-Generation Netw. (IJNGN)*, vol. 1, no. 1, 2009.

[11] S. K. Singh, M. P. Singh, and D. K. Singh, "A survay of energy-efficient hierarchical cluster-based routing in wireless sensor networks", *Int. J. Adv. Netw. Appl.*, vol. 2, no, 2, pp. 570–580, 2010.

[12] S. K. Singh, M. P. Singh, and D. K. Singh, "Energy-efficient homogenous clustering algorithm for wireless sensor networks", *Int. J. Wirel. Mob. Netw.*, vol. 2, no. 3, pp. 49–61, 2010.

[13] ZigBee Alliance, "ZigBee Specification v1.0", New York, USA, 2005.

[14] M. I. Shukur, L. S. Chyan, and V. V. Yap, "Wireless sensor networks: delay guarantee and energy efficient MAC protocols", *World Academy of Sci., Engin. Technol.*, vol. 50, pp. 1061–1065, 2009.

[15] N. Sastry, D. Wagner, "Security consideration for IEEE 802.15.4 networks", in *Proc. 5th Int. Conf. Web Inform. Sys. Engin. WISE 2004*, Brisbane, Australia, 2004, pp. 32–4.

[16] R. Struik and G. Rason, "Security and security architectural recommendations for the IEEE 802.15.4 Low-Rate WPAN", Certicom Corp., 2002.

[17] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks", *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, 2002.

[18] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", in *Proc. 2nd Int. Conf. Embedded Networked Sensor Sys.*, Baltimore, MD, USA, 2004, pp. 162–175.

[19] L. E. Lighfoot, J. Ren, and T. Li, "An energy efficient link-layer security protocol for wireless sensor networks", in *Proc. IEEE Int. Con. Elec.-Infor. Technol. EIT 2007*, Chicago, IL, USA, 2007, pp. 233–238.

[20] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", in *Proc. 10th ACM Conf. Comp. Commun. Secur. CCS 2003*, Washington, DC, USA, 2003, pp. 62–72.

[21] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks", *ACM Trans. Sensor Netw. TOSN*, vol. 2, no. 4, pp. 500–528, 2006.

[22] H. Cam, S. Ozdemir, D. Muthuavinashiappan, and P. Nair, "Energy efficient security protocol for wireless sensor networks", in *Proc. IEEE 58th Veh. Technol. Conf. VTC 2003*, Orlando, Florida, USA, 2003, vol. 5, pp. 2981–2984.

[23] R. A. Shaikh, S. Lee, M. A. U. Khan, and Y. J. Song, "LSec: lightweight security protocol for distributed wireless sensor network", *Lecture Notes in Computer Science*, vol. 4217, 2006.

[24] T. Shon, B. Koo, H. Choi, and Y. Park, "Security architecture for IEEE 802.15.4-based wireless sensor network", in *Proc. 4th Int. Symp. Wirel. Pervasive Comput. ISWPC 2009*, Melbourne, Australia, 2009, pp. 1–5.

[25] A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", *Annales des Telecomm.*, pp. 529–541, 2008.

[26] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", in *Proc. 33rd Annual Hawaii Int. Conf. Sys. Sciences HICSS'00*, Maui, Hawaii, USA, 2000, pp. 3005–3014.

[27] B. Azzedine, C. Xiuzhen, and J. Linus, "Energy-aware datacentric routing in microsensor networks", in *Proc. 6th Int. Symp. Model. Analys. Simul. Wirel. Mobile Sys. MSWiM 2003*, San Diego, CA, USA, 2003, pp. 42–49.

[28] K. Lin, Ch. F. Lai, X. Liu, and X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks", *Mob. Netw. Appl.*, vol. 17, pp. 75–89, 2012.

[29] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks", in *Proc. 25th IEEE Int. Conf. Com. Commun. INFOCOM 2006*, Barcelona, Spain, 2006, pp. 1–12.

[30] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks", in *Proc. Worksh. Real-World Wirel. Sensor Netw. REALWSN'05*, Stockholm, Sweden, 2005, pp. 1–5.

**Krzysztof Daniluk** received his M.Sc. in Computer Science from the Trinity College Dublin, The University of Dublin, in 2010 and Polish-Japanese Institute of Information Technology, Warsaw, in 2010. Currently he is a Ph.D. student in the Institute of Control and Computation Engineering at the Warsaw University of Technology. His research area focuses on wireless sensor networks, energy-efficiency together with security issues, computer networks.
E-mail: K.Daniluk@stud.elka.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

**Ewa Niewiadomska-Szynkiewicz** – for biography, see this issue, p. 38.