SECURITY IN WIRELESS SENSOR NETWORKS

Assist. Prof. Aleksandar Ivanov, PhD
Burgas Free University

Abstract: *Wireless sensor networks are developing technology for environment observation. These networks can provide infrastructure for monitoring and control of both outdoor and indoor facilities and increase security, on both technical and human level. They are one of the most useful implementations of IoT. Security in sensor networks is a cricital issue. In this paper a brief overview of security instruments for wireless sensor neworks is presented.*

Keywords: *wireless sensor networks, security*

I. Wireless sensor networks

Wireless Sensor Networks – WSNs, are ad-hoc networks of sensors for monitoring the physical features of the environment such as humidity, temperature, chemical substances, lumosity, pressure, etc. The sensors are typically attached to walls, ceilings, roofs or special installments in different facilities, both indoors and outdoors. They communicate using wireless radio signals. WSNs operate in a resource constrained environment and therefore deviate from the traditional OSI model. They are usually decentralized ad-hoc networks. Usually WSNs contain one or several sink nodes (cluster heads) that collect data from cluster groups that generate it. Ad-hoc refers to the property of instantaneous flexible configuration of the network as opposed to predefined wiring and topology constraints.

This type of networks represents a typical application of Internet of Things (IoT) and they have variety of use-cases – monitoring storage units, monitoring power plants, automated agriculture, smart cities, monitoring structural integrity of buildings, medical tracking, disaster prevention and others. In the context of ESG (Environmental, Social, Governance) factors in economy, WSNs can be useful in all three aspects. In terms of environment monitoring and control, WSNs can be deployed to monitor environmental parameters such as air quality, water quality, noise levels, and temperature. By collecting and analyzing this data, organizations can gain insights into the impact of their operations on the environment. This information can be used to drive sustainable practices and reduce the environmental footprint. By deploying sensors in buildings, factories, or agriculture fields, organizations can monitor resource usage, detect inefficiencies, and optimize consumption patterns. This data-driven approach can lead to better resource allocation and reduced waste. WSNs can be employed to track and monitor supply chains, ensuring compliance with ESG standards. Sensors can be integrated into products or packaging to monitor their location, condition, and adherence to ethical and sustainable sourcing practices. This level of transparency enables organizations to make informed decisions about their supply chains and promote responsible sourcing. In the social aspect, WSNs can contribute to social impact initiatives by enhancing safety and well-being. For example, in smart cities, WSNs can monitor traffic flow, detect accidents, and improve emergency response times. In healthcare, wearable sensor networks can

assist in remote patient monitoring, enabling personalized care and reducing hospital visits. These applications improve the quality of life and promote social well-being. WSNs can also assist in monitoring and compliance efforts related to ESG regulations and standards. By collecting data on emissions, waste management, or occupational health and safety, organizations can ensure compliance with relevant guidelines and benchmarks.

By deploying WSNs in industrial facilities one can provide more security on all levels. Monitoring the parameters of the environment can be the basis for automated machine control. By monitoring the facilities human intrusion can also be detected in real-time. To achieve these goals it is crucial to make a network itself secure. In the next sections a brief overview of security measures in WSNs is presented.

II. Security concerns in wireless sensor networks

WSNs are vulnerable to various security threats due to their inherent characteristics - limited resources, distributed nature, and wireless communication. There are different aspects of security when deploying WSNs. The threats for a WSN can be on control level. WSNs are vulnerable to various types of attacks, such as Byzantine attack, man-in-the-middle, DDoS, Sybil, etc. Attacks can also be aimed at recoinnaissence – the gathering of information for future planning of larger attack. Here are some important security concerns regarding WSNs:

- *Secure Communication*: Transmisssion of collected data to a central source needs secure communication. Using encrypted data transfer ensures that data transmitted over the wireless medium cannot be easily intercepted by unauthorized entities. Key management is important part of securing WSN communications.
- *Authentication and Access Control*: Sensor nodes should be equipped with authentication mechanisms to verify the identity of other nodes or users before allowing access to the network. Access control mechanisms can be implemented to enforce authorization policies and restrict unauthorized access to the network and its resources.
- *Secure Data Aggregation*: In WSNs, data aggregation is often performed to reduce the amount of transmitted data and conserve network resources. Data aggregation techniques should be employed to prevent malicious nodes from injecting false data into the aggregated results.
- *Intrusion Detection and Prevention*: Intrusion detection systems can be deployed in WSNs to detect and respond to any malicious activities or anomalies. Signature-based and anomaly-based intrusion detection techniques can be used to identify potential attacks and trigger appropriate countermeasures in response to the threats.
- *Energy-Efficient Security*: Since sensor nodes in WSNs have limited resources, security mechanisms should be designed to be energy-efficient. Some solutions are energy-aware protocols (GEAR, S-HERS, D-HERS, MLDA) [1], lightweight encryption algorithms, and low-power cryptographic primitives, all aimed at minimizing the energy consumption of security operations. Real-time monitoring can be critical in some use-case scenarious and reliable energy supply should be provided.
- *Physical Security:* Physical security measures, such as tamper-resistant packaging for sensor nodes and secure deployment of nodes in inaccessible locations, can help prevent physical attacks and unauthorized access to the network. It is also important to protect the sensors from disruptive elements in the environment, such as oxydation, moist, radio interference, etc. To prevent radio interference or jamming,

the two common techniques used are frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS).[2]

- *Secure Routing*: Its aim is to protect against routing attacks, including packet dropping, routing table poisoning, and selective forwarding. Software should always be up-to-date and maintained regularly. Security patches and updates should be installed as soon as possible.
- *Privacy Preservation*: In applications where privacy is a concern, techniques such as data anonymization, data perturbation, or secure multiparty computation can be employed to protect sensitive information and prevent unauthorized disclosure.
- *High availability:* network operation should not be dependent on particular nodes. Critical nodes should have duplicates. There should also be path redundancy in communication.

It's important to note that the choice and implementation of security measures in a WSN depend on the specific application requirements, available resources, and expected threats. The security solutions should be tailored to address the unique challenges and constraints of a particular wireless sensor network.

III. Encryption in wireless sensor networks

In WSNs there can be different types of data collected – sensory readings (usually numerical data), image and video data, audio data, location data. Sensory readings may be recorded values of periodically monitored variables or detected events – usually changes or anomalies in the environment. Data from multiple sensors can also be summirized to reduce its volume. Data formats are usually protocol-specific. Plaint text, JSON and XML formats are possible choices for data formatting. To safely transmit data across multiple devices in the network, the use of encryption is recommended.

Encryption typically uses strings serving as keys to replace characters in the original data. There are two main types of encryption algorithms – symmetric and assymetric. Symmetric algorithms use the same key for both encryption and decryption. Assymetric algorithms use different keys (a pair of a public and a private key) for these tasks. Here is a list of some encyption algorithms:

- *Advanced Encryption Standard (AES):* AES is one of the most used symmetric encryption algorithms. It offers different key sizes (128, 192, or 256 bits). AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. It can be efficiently implemented on resource-constrained sensor nodes. There is no known practical attack that would allow someone without knowledge of the key to read data encrypted by properly implemented AES.

- *Tiny Encryption Algorithm (TEA)*: TEA is a lightweight symmetric encryption algorithm designed specifically for low-power devices. It is a block cipher with 128-bit keys that can be implemented with just a few lines of code. It is preferred when minimal computational resources should be used.
- *Rivest Cipher (RC) Algorithms*: The RC family of symmetric encryption algorithms uses stream ciphers where plain text digits are combined with pseudo-random digits. There are several implementations such as RC4 and RC5, that have been used in WSNs due to their simplicity and efficiency. However, some of these algorithms, like RC4, have security vulnerabilities that should be considered.
- *Elliptic Curve Cryptography (ECC)*: ECC is a public key cryptography algorithm that provides strong security with shorter key lengths compared to

traditional algorithms like RSA. ECC is well-suited for resource-constrained devices in WSNs due to its computational efficiency.

- *RSA (Rivest-Shamir-Adleman)*: RSA is a widely used public key (assymetric) cryptography algorithm. It is based on prime number factorization. While it offers strong security, it is computationally intensive, which makes it less suitable for resource-limited sensor nodes. However, RSA can be used for key exchange and digital signatures in WSNs.
- *Diffie-Hellman (DH*): The Diffie-Hellman key exchange protocol allows two parties to establish a shared secret key over an insecure channel. It can be used in combination with symmetric encryption algorithms to securely exchange keys in WSNs. It is one of the oldest public key algorithms.
- *Pairing-Based Cryptography (PBC)*: PBC is a type of public key cryptography that is efficient for resource-constrained devices. It is particularly useful in scenarios where secure communication and key agreement are required. Pairing-based cryptography is based on pairing functions that map pairs of points on an elliptic curve into a finite field. [3]
- *Lightweight Cryptography*: Several lightweight encryption algorithms and protocols, specifically designed for constrained devices, have been proposed for use in WSNs. Examples include PRESENT, SIMON (hardware-oriented), and SPECK. These algorithms can provide sufficient security while minimizing resource requirements. [4]

As it was mentioned before, the choice of encryption protocols should be aligned with other factors such as computational complexity, memory requirements, energy consumption, and the level of security needed for the application.

IV. Routing in WSNs

Routing in WSNs is a non-trivial matter because a WSN require low-energy consuming, fast and simple routing protocols performed by sensors instead of dedicated routers.[2] Routing in WSNs can be classified in two main strategies – datacentric and address-centric. In datacentric strategies the focus is on aggregating the data instead of tracking its source. Data-centric routing utilizes attributes or properties associated with the data to guide the routing process. Examples include data attributes such as data type, data relevance, or data aggregation. Examples of data-centric routing protocols include SPIN (Sensor Protocols for Information via Negotiation) and Directed Diffusion. Datacentric approaches are more energy-efficient. Address-centric routing is primarily concerned with the location or addressing information of the nodes in the network. Address-centric routing assigns unique addresses or identifiers to each node in the network, and routing decisions are made based on these addresses. Routing protocols in WSN can be broadly classified into proactive, reactive, hybrid, and location-aware routing protocols. Proactive routing protocols, also known as table-driven protocols, establish and maintain routing information continuously, regardless of whether there are active data transmission needs. Reactive routing protocols, also known as on-demand protocols, establish routes on an as-needed basis. When a node wants to send data to a destination, it initiates a route discovery process. Hybrid routing protocols combine elements of both proactive and reactive protocols to leverage their advantages. They maintain routing information for frequently communicating nodes proactively while establishing routes on demand for other nodes. Location-aware routing protocols utilize location information of the network nodes to make routing decisions. Each

node in the network knows its geographical coordinates and can use this information to determine optimal paths based on distance or other location-based metrics.

Encryption can be used not only to encrypt sensory readings, but also in routing protocols. Several routing protocols were specifically designed for WSNs. They provide secure ways to transmit data between nodes.

Destination Sequenced Distance Vector (DSDV) routing protocol is a routing protocol commonly used in mobile ad-hoc networks (MANETs) and, to some extent, in WSNs. It is based on Bellman-Ford routing algorithm and it is similar to RIP. Some key characteristics and features of the DSDV routing protocol are: proactive routing, which means that nodes maintain and update routing information continuously, regardless of whether there are active data transmissions. DSDV uses sequence numbers to determine the freshness of routing information.

Ad-hoc On-Demand Distance Vector (AODV) routing is the routing protocol used in Zigbee – a low power, low data rate wireless ad-hoc network. There are various implementations of AODV such as MAD-HOC, Kernel-AODV, AODV-UU, AODV-UCSB and AODV-UIUC. [5] AODV is an on-demand routing protocol that establishes routes only when they are needed. Nodes maintain route information only for active communication sessions. When a node wants to send data to a destination node and has no valid route, it initiates a route discovery process. Route requests (RREQ) are broadcasted to neighboring nodes to find a route to the destination. AODV utilizes periodic route maintenance to monitor the connectivity of established routes. If a route becomes invalid or breaks, the affected nodes trigger a route error (RERR) message to inform other nodes about the broken link. Each node in AODV maintains a routing table that stores information about the destination nodes, next-hop nodes, hop counts, and sequence numbers to determine the freshness of routing information. AODV employs sequence numbers to avoid routing loops. Nodes discard or ignore routing information with lower sequence numbers, preventing loops in the network. [6]

Dynamic Source Routing (DSR) is a source routing protocol where the entire route from the source to the destination is included in the packet header. Each node forwards the packet based on the source-specified route. It involves two processes – route discovery and route maintance. Route Discovery occurs when a node wants to send data to a destination, but the route is unknown. Route requests (RREQ) are flooded in the network, and nodes that receive the request cache the route information for future use. DSR relies on route caching, where intermediate nodes store recently used routes. Cached routes can be used to satisfy future route requests without performing route discovery again. DSR includes route maintenance mechanisms. If a link fails or a route becomes invalid, the source node is notified through a route error (RERR) message, allowing it to reattempt route discovery. DSR is an on-demand (reactive) protocol designed to restrict the bandwidth consumed by control packets in ad-hoc wireless networks. [7]

The Zone Routing Protocol (ZRP) is a hybrid routing protocol designed for wireless ad-hoc networks, including WSNs. It combines the advantages of both proactive and reactive routing protocols to achieve efficient and scalable routing. ZRP employs a hybrid routing approach by dividing the network into zones. It combines proactive routing within a local zone and reactive routing between zones. This allows for efficient routing within a zone while minimizing the overhead associated with maintaining routing information for the entire network. In ZRP, the network is divided into a series of zones, with each zone having a designated zone coordinator. The zone coordinator is responsible for maintaining routing information within its

zone. Within each zone, ZRP uses a proactive routing protocol, such as Intra-zone Routing Protocol (IARP), also using Neighbor Discovery Protocol, to maintain up-to-date routing information. Proactive updates occur within the zone to establish and maintain routes between nodes. When a node wants to communicate with a node outside its zone, ZRP switches to reactive routing. It uses a route discovery process according to Inter-zone Routing Protocol (IERP), to find a route to the destination. This process involves flooding route requests or utilizing route caching mechanisms. Border nodes act as gateways between different zones. They maintain routing information for adjacent zones and facilitate inter-zone communication. ZRP adjusts the size of zones dynamically based on the network's density and topology changes. This allows for flexible adaptation to network dynamics, improving scalability and reducing control overhead. ZRP incorporates mechanisms for route maintenance and repair to handle node failures or topology changes. When a link or node fails, ZRP detects the failure and triggers the necessary actions to repair or update routes affected by the failure. [8]

Geographic- and Energy-Aware Routing (GEAR) is a routing protocol specifically designed for WSNs, that takes into account both geographic location and energy considerations in making routing decisions. GEAR aims to improve energy efficiency and prolong network lifetime by leveraging the knowledge of node positions and their energy levels. In GEAR, each sensor node is aware of its geographical coordinates and energy status. The protocol employs a combination of geographic and energy-aware metrics to select routes and forward data packets towards the destination. It uses an energy aware neighbor selection and forwards the packet in recursive manner. [9]

SHARP (Secure Hop-by-Hop Authentication with Efficient Revocation Protocol) is a secure hybrid routing protocol. SHARP enables application-specific adaptation strategies to bound loss rate, in addition to controlling the overhead of the routing protocols [10]. **LEACH (Low Energy Adaptive Clustering Hierarchy)** is an energy-efficient clustering-based routing protocol widely used in WSNs. LEACH is a hierarchical routing protocol where the sink node in a cluster changes stochastically at each round of data communication. LEACH can be extended with additional security mechanisms. These extensions may include the use of cryptographic algorithms for secure communication between cluster heads and sensor nodes, secure key management, and intrusion detection mechanisms. Using LEACH may lead to uneven distribution of cluster heads and energy exhaustion of particular nodes. [11]

Apart from these specific protocols, other secure routing protocols have been proposed for WSNs, including TinySec and SPINS. **TinySec** is a security framework designed specifically for resource-constrained wireless devices, including WSNs. The algorithm works on the data-link layer of the network and it is part of the official TinyOS release. TinySec utilizes lightweight encryption algorithms suitable for resource-constrained devices. It ensures message integrity through the use of message authentication codes (MACs). TinySec is designed to minimize computational and communication overheads to suit the limited resources of sensor nodes. It employs optimized algorithms and protocols to reduce the energy consumption and processing requirements during security operations. It provides a transparent security layer that can be utilized by higher-level protocols without significant modifications. The algorithm offers a balance between security and resource efficiency, making it suitable for applications where lightweight security is required. [12] **SPINS (Security Protocols for Sensor Networks)** is a suite of security protocols specifically designed

for WSNs. It consists of several protocols that address different security aspects in WSNs, including secure communication, key management, and time synchronization. Here's an overview of the key protocols included in the SPINS suite:

- SNEP (Sensor Network Encryption Protocol): SNEP provides secure communication between sensor nodes in a WSN. It utilizes symmetric encryption algorithms to ensure confidentiality and integrity of the transmitted data. SNEP also incorporates methods for key distribution and establishment among sensor nodes. [13]
- µTESLA (Micro Timed Efficient Stream Loss-tolerant Authentication): µTESLA is a time synchronization and message authentication protocol. It allows sensor nodes to synchronize their clocks efficiently while providing message authenticity and integrity. µTESLA is designed to be energy-efficient and robust against timing attacks. [14]

The SPINS suite of protocols is specifically tailored for the unique requirements and constraints of WSNs. It emphasizes lightweight cryptographic algorithms, energy efficiency, and scalability. The suite offers a comprehensive set of security protocols that work together to address various security aspects in WSNs, such as data confidentiality, integrity, authentication, time synchronization, and key management.

PEGASIS (Power-Efficient Gathering in Sensor Information Systems) is a chain-based hierarchical routing protocol that forms chains of nodes to transmit data to the base station. It aims to reduce energy consumption through data aggregation and cooperative communication.

V. Conclusion

WSNs can provide security solutions for great variety of industrial and public facilities and installments. These networks can automate some basic security responses based on events and patterns in collected data. When designing such a solution in practice, security of nodes and their communication should be a major concern. There are various encryption and hardware measures that can make WSNs secure. When deployed in an efficient manner these tehniques can ensure the stable operation of both the sensory networks and the monitored environments.

Bibliography:

1. Yang, D., Li, X., Sawhney, R., & Wang, X.. Geographic and energy-aware routing in Wireless Sensor Networks. IJAHUC. 4. 61-70. 10.1504/IJAHUC.2009.023897., 2009
2. Dubrawsky, I., Chapter 6 - Wireless Networks,, *Eleventh Hour Security+, Syngress,* 2010, Pages 77-88, ISBN 9781597494274, https://doi.org/10.1016/B978-1-59749-427-4.00006-X.
3. Szczechowiak, P., et al., On the application of pairing based cryptography to wireless sensor networks, *Proceedings of the second ACM conference on Wireless network security*,Pages 1–12, https://doi.org/10.1145/1514274.1514276, 2009
4. Suzaki, T., Minematsu, K., Morioka, S., and Kobayashi, E., TWINE: A lightweight block cipher for multiple platforms, *SAC* 2012.
5. Jhaveri, R.H.; Patel, N.M. (2015). Mobile Ad-hoc Networking with AODV: A Review. *International Journal of Next-Generation Computing*. **6** (3): 165–191.
6. https://www.ietf.org/rfc/rfc3561.txt
7. https://datatracker.ietf.org/doc/html/rfc4728

8. Yang, X., Chen, Q., Chen, Z., Zhao, J., Improved ZRP Routing Protocol Based on Clustering, *Procedia Computer Science*, Volume 131, 2018
9. Srivastav , G., Effective Sensory Communication using GEAR Protocol, *International Journal of Science and Research (IJSR),* ISSN (Online): 2319-7064, 2013
10. Zygmunt J. Haas, Emin Gun Sirer., SHARP: A hybrid adaptive routing protocol for Mobile ad-hoc networks, 2003
11. Akkaria, W., Bouhdida, B., Belghithb, A., LEATCH: Low Energy Adaptive Tier Clustering Hierarchy, *6th International Conferenceon Ambient Systems,* Networks and Technologies, DOI: **10.**1016/J.PROCS.2015.05.110, 2015
12. Karlof, C., Sastry, N., Wagner, D., (2004). TinySec: A link-layer security architecture for wireless sensor networks. *SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems.* 162-175. 10.1145/1031495.1031515. Ramasubramanian, *In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc)*, 2003.
13. Tobarra, Ll., Cazorla, D., Cuartero, F. Formal Analysis of Sensor Network Encryption Protocol (SNEP). 1-6. 10.1109/MOBHOC.2007.4428763., 2007
14. Perrig, A., Canetti, R., Tygar, J., Briscoe, B... Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction. *Internet Requests for Comments*. *RFC 408*2., 2005