Threats to Wireless Sensor Networks and Approaches to Use Homomorphic Encryption to Secure Its Data

Ludmila Babenko and Ekaterina Tolomanenko*
Southern Federal University, Institute of Computer Technology and Information Security, Taganrog, Russia

*Corresponding author email: kat.tea@mail.ru

Abstract. The article considers the basic principles of building modern wireless sensor networks. The general structures of such networks, their application spheres, their strengths and weaknesses are considered. Special attention is paid to the problem of security of processed and transmitted data, as well as existing approaches to providing reliable cryptographic protection of these data in wireless sensor networks. It is shown that at working out of mechanisms of maintenance of protection of the information in sensor networks first of all it is necessary to consider restrictions inherent in such networks on volume of memory, speed of used processors, and also power consumption. This leads to a more careful and weighted choice of encryption algorithms for use in sensor networks, both for direct encryption of data collected and transmitted by sensor networks nodes, and for auxiliary functions such as calculating the optimal network route by routers that are part of sensor networks. The article focuses on the possibility of using homomorphic encryption systems to protect data collected by sensors and transmitted via wireless connections. The advantages of full and partial homomorphic encryption systems in terms of their application to sensor networks with sensors measuring environmental parameters are shown. The analysis showed that using partial homomorphic encryption over the Paye Cryptosystem to hide data in sensor networks had reasonable grounds.

1. Introduction
WSN, or Wireless sensor networks are usually groups of separated in space dedicated sensors that have the means to receive and transmit information (or only transmission). These groups of sensors are used to record and monitor the physical conditions of their environment, and to organize the collection of all received data in one place. Examples of environmental conditions may include temperature, humidity, noise level, pollution, wind speed, etc.

Wireless sensor networks are built from nodes, small all-in-one devices — usually called sensor motes, from a few to hundreds and thousands of sensors, each connected to another or more sensors. Every such mote usually consists of several parts: a small power source (battery or power generation system), a microcontroller with built-in memory chips and cache, one or few sensors, an electronic circuit to interface with the installed sensors, and a radio transmitter with an internal antenna or connection to an external antenna. The power source is usually a miniature battery, or a circuit with an integrated form of energy collection (wireless charging). The size of a single device can range from a small box to barely visible devices, although devices of this microscopic size do not yet exist as industrial designs.

In addition to inexpensive and miniature motes, sensor networks usually include so-called base stations. The base stations are single or multiple components of wireless sensor networks, but in contrast to motes, they have much more computing, energy and communication resources. They...
usually act as a gateway between the sensor nodes and the end user, since their purpose is to transfer data from WSN to a central server. Other special nodes in networks based on data packet routing are routers, which is designed to calculate and distribute routing tables. [1]

Another important parameter of sensor networks is the operating systems (OS) used in motes. Of course, the complexity of such operating systems does not compare to general-purpose operating systems, rather, they are closer to the embedded OS. The reasons for this are primarily because wireless touch networks are usually designed for a specific purpose and application rather than for general use. Secondly, one should not forget about the low cost and extremely low power consumption of WSN nodes, which forces the use of special microcontrollers in their hardware, with low power consumption, and therefore with limited functionality and memory capacity. This imposes serious limitations on the complexity and size of operating systems for wireless touch networks. Examples of operating systems designed specifically for wireless touch networks are TinyOS, LiteOS, Contiki and others. Most of these operating systems are event-programmable, not multithreaded, as their "older" counterparts. In doing so, they support the C programming language, which makes it easier to develop applications and event handlers from sensors in these operating systems.

As in any distributed systems that process information, data protection from third parties' encroachments is not the least important in wireless sensor networks. Developers of such systems are compelled to balance between temptation to use persistent algorithms of data encryption and restrictions of productivity, power consumption and volume of the built in memory of motors. Most of them prefer the usual symmetric or asymmetric data encryption algorithms, but there are algorithms that can offer wireless touch networks an unrivalled level of convenience - homomorphic encryption algorithms. In given article the concrete partially homorphic algorithm of encryption of the data - cryptosystem PAYE which will allow to reduce superfluous expenses for constant data encryption at each stage of data transfer from sensors to base stations will be offered.

The article is organized as follows. Section 2 deals with the main threats to wireless sensor networks from malicious users trying to steal data transmitted from the moth to the base station, while section 3 discusses existing approaches to data protection in such networks using symmetric and asymmetric encryption. Also in section 3 it is offered and proved the possibility of application of partially homomorphic cryptosystem PAYE for convenient operation over the transferred data without the necessity of data encryption operation in each cycle of data transmission through open communication channels. Finally, section 4 presents our conclusions.

2. Threats to Wireless Sensor Networks

For all its advantages, wireless touch networks have more obvious security concerns than traditional wired networks. Thus, in particular, the network architecture of sensor networks (Mesh network topology), common features of their application (isolation, autonomy) can often result in the appearance of weaknesses in the integrity of both the entire wireless network and individual computers. Because of the unique characteristics of wireless sensor networks, traditional methods of securing computer networks are useless (or less effective) for them, because an attacker knows a priori that the nodes of a wireless sensor network constantly exchange information with each other. Consequently, the lack of security mechanisms will lead to intrusion attempts on such networks. These intrusions need to be identified and mitigation techniques applied.

The most common types of network attacks on wireless sensor infrastructure are the following:

1. Denial of Service attack (DoS-attack) — The main purpose of such attacks is to overload the sensor or base station with requests so that the attacked host of the wireless sensor network becomes inaccessible to authorized users and other network hosts. [2] Basically, this is achieved by sending a huge number of network packets that do not carry much meaning, and as a result the network node is no longer able to receive normal network packets (Figure 1).

2. Sinkhole attack — In this attack, the attackers register a new host on the wireless sensor network that makes itself attractive to surrounding hosts using false routing information. At the same time, all data destined for the base station passes through this malicious host using a high quality route. It then makes a change or selective redirection of the data. [3] Figure 2 shows a diagram of such an attack on a wireless sensor network, where the pink color
indicates hosts that use a high-performance but malicious host to transmit data and the green color indicates hosts that are not affected by the attackers.

Figure 1. DoS attack in WSN  
Figure 2. Sinkhole attack in WSN

3. A Wormhole attack is essentially a partnership attack in which the attackers can act together to fake the target node. This is the most serious attack on wireless sensor networks. This attack also uses a high-speed subnet. The source sends data that is falsely transmitted through the attacker's zone. The attacker or malicious hosts then passes the data to the destination over a high-speed link faster than any other link from source to destination. Because requests are received more quickly via a false high speed link, the destination host also chooses the same path to send its response. When responses arrive at the source through the source node of the attack zone, the destination node also begins sending its data on a path that includes the attacking nodes without knowing it. The result is that all of the data goes through the malicious hosts. [4] Figure 3 shows a schematic representation of the moles being included in an existing wireless sensor network.

Figure 3. Wormhole attack in WSN

4. Passive data collection — for this attack the attacker uses a powerful receiver and a well-designed antenna to intercept the data stream transmitted to and from the wireless sensor network. In this case, most of the information is easily accessible to the attacker and can be used for further direct attacks on the network in the event that the data is transmitted openly. This method also makes it possible for an attacker to detect and destroy sensors on the network.

Because sensor networks are constantly exchanging data over poorly secured wireless communication channels, this data needs to be protected if it is valuable. However, the limitations imposed by the very nature of sensor networks, such as low microprocessor power, low memory capacity and limited energy resources, should be taken into account when developing methods to protect information in sensor networks. Another problem that complicates the development of information security mechanisms in wireless sensor networks is the fact that sensor network motes operating in difficult conditions (weather or other) can often lose contact with neighboring nodes, so they will break up and reestablish connections with neighboring devices. Therefore, one of the main problems in building secure WSNs is to ensure the security of transmitted data, which, however, should not be achieved at the expense of the miniaturization and low power consumption of the motes.

3. Securing WSN Data
There are several terms that are directly related to data security in computer networks. **Authentication** is the process of confirming the identity of parties involved in the messaging process. **Confidentiality** describes the process of protecting transmitted data in such a way that it is not disclosed to a third party under any circumstances. **Data Integrity** means that data is not replaced or changed by someone during transmission. The term **Key management** refers to the cryptographic
domain and describes the management of encryption keys: creation, storage, sharing, use and replacement of encryption keys.

Some security vendors prefer to invest in Intrusion detection systems (IDS) rather than in quality data protection. Intrusion detection is performed either at the hardware level, using special devices or at the software level, using algorithms for traffic analysis, suspicious activity and attempts to violate security policies. However, for wireless sensor networks, such algorithms are not very applicable, given the limitations inherent to WSN nodes.

In order to avoid the attacks described in Section 2 and to achieve the security of data transmitted by WSN, the architects of such systems often lay the use of some cryptographic algorithms as the cornerstone of the WSN security architecture. At the same time, encryption algorithms meet all basic requirements for data security: confidentiality, integrity and indivisibility. For data protection in WSN usually use only 2 types of cryptography algorithms: cryptography with one secret key (Symmetric Cryptography) and cryptography with two keys, private and public (Asymmetric Cryptography). These two types are fundamentally different in their data manipulation schemes. [5]

3.1. Symmetric and Asymmetric Cryptosystems in Wireless Sensor Networks
Symmetric cryptography algorithms encrypt and decrypt data with the same key, which must be kept strictly confidential. It is the task of keeping the key secret from third parties that is the main one when using such encryption algorithms, despite their relatively low complexity. [6] The most known and frequently used are symmetric encryption algorithms such as AES, DES, RC4, RC5, CAST. [7,8,9,10] Asymmetric cryptography algorithms operate with two different, despite related to each other, keys — public and secret. The secret key never appears on the network in plain sight. Due to the fact that in asymmetric encryption algorithms encryption keys are never transmitted over the network, security developers are able to avoid high-level attacks on the network infrastructure, thus providing a sufficient level of security with relatively little effort. [11] However, despite its great popularity, asymmetric encryption algorithm RSA is not the most effective and low-cost method of encrypting data in WSN, according to [12]. In this work the authors have compared the implementation of algorithms ECC-160, ECC-224 and RSA-1024 in the emulator WSN. As the results of their research showed, the implementation of cryptography based on RSA algorithm requires a little more effort to implement security requirements than ECC-224, which provides more appropriate solutions in terms of time and power consumption.

But, as shown in [13], the use of public-key cryptography on small wireless devices is provided solving for reliable and efficient authentication and key exchange protocols requirements.
So, using this basis, we can conclude that not every encryption algorithm is suitable for use in wireless sensor networks. Some encryption algorithms require a lot of memory for their work, others are very dependent on the performance of the microprocessor used, and some need much time, spending a lot of energy on data encryption.

3.2. Approaches to Use Homomorphic Cryptography in WNSs
The main important feature of wireless sensor networks is the use of mesh network topology, using which network data is transmitted via radio channel in all directions and anyone can receive it. Optimal route of packets passing is calculated by time of information passing from sender to receiver and back. The addresses of the intermediate sections of the wireless network with the highest speed and bandwidth form the data route. In the case of wireless sensor networks, the optimal scheme would be a scheme where the addresses of all the motes are known in advance and the network modules build the routes from the previously known addresses. With this approach, the risks of embedding attacker nodes in a wireless sensor network can be minimized. The only problem remains the need to hide the network address pool from attackers so that they cannot add their devices with the eligible network addresses.

To solve this problem, homomorphic encryption can be used, which is embedded in routing protocols to improve security. In this case, operations on the encrypted data can be securely performed by intermediate hosts. In particular, one of the main tasks of routing - to find the optimal path between
two nodes of the network, it is necessary to perform certain linear operations on encrypted data, without resorting to decryption and subsequent encryption. In this case, using partially or completely homomorphic encryption will not allow the third party to find any connection between messages received by the WSN host and messages sent by the host further, since absolutely all data is always in encrypted form. Consequently, the task of tracing the path of the messages through traffic analysis will also become unsolvable. [14] It is possible to go even further, and by slightly improving the network drivers running in the motes, to ensure that absolutely all of the data is transmitted in encrypted form — both the network packet headers and the contents. With homomorphic encryption, network drivers will be able to modify network addresses of packets without having to perform a costly operation of decrypting and then encrypting network packet header data.

As an encryption algorithm that supports homomorphism, it is useful to use the PAYE Cryptosystem because it is additively homomorphic, i.e. it allows adding and multiplying operations on ciphers that correspond to similar operations on open text. [15]

3.3. Homomorphism of PAYE Cryptosystem

Thus, in the PAYE Cryptosystem, the multiply of two ciphers will be deciphered as the sum of their corresponding open texts:

\[
D(E(m_1, r_1) \ast E(m_2, r_2) \mod n_2) = m_1 + m_2 \mod n.
\]

By multiplying the ciphertext by \(g^{m_2}\) we will get the sum of the corresponding open texts:

\[
D(E(m_1, r_1) \ast g^{m_2} \mod n_2) = m_1 + m_2 \mod n.
\]

In (1) and (2) \(m_1\) and \(m_2\) are open texts, \((n, g)\) — is a pair of two numbers, that forms open key, \(r_1\) and \(r_2\) — two random numbers, \(E\) is the encryption function, and \(D\) is the decryption function.

3.4. Practical use of Homomorphic PAYE Cryptosystem in WSN

In order to minimize computing and time resources for the practical use of the proposed approach in wireless sensor networks, in particular in networks using environmental sensors, it is proposed to take as \(m_1\) the basic and invariable value of the measured parameters, and as \(m_2\) the precalculated and encrypted numerical values, which will correspond to an increase (in case of positive values) or decrease (in case of negative values) of the measured parameters. Of course, this will require more memory for the motes to store the entire array of encrypted numerical values, but given the current state of affairs in the field of memory chip production, the constant reduction of memory cells size and their price, while increasing the volume, this should not be a problem. At the same time, this approach will radically reduce the time, as well as the power consumption, required to prepare an encrypted network message on the low-power mot's side.

Since the arithmetic operation on the encrypted data will only be done once, and in the next cycle of sending will start over, this will avoid the accumulation of the error inherent in all partially homomorphic encryption systems.

4. Conclusion

Thus, the information reviewed suggests that symmetric cryptography is less suitable for use in WSN than asymmetric cryptography. In addition to key management and security, public key cryptography can be an efficient and reliable scheme for the number of WSN applications. Public key cryptography offers more advantages due to low memory usage, low CPU consumption, and the size of the key provides better protection than symmetric encryption algorithms. In addition, homomorphic cryptosystems such as the PAYE cryptosystem can offer an additional benefit of unprecedented ease of use in that there is no need to re-encrypt data when little change is made to the data being transmitted, such as when transmitting measurements of temperature, pressure and similar physical quantities. Instead, the encrypted value of the measured parameter change is added or multiplied with the encrypted value of the same parameter in the previous measurement step. This allows the number of information encryption cycles to be significantly reduced, which means that the power consumption of the mot is reduced and the battery life of the mot is extended for a long time.
Acknowledgement
The reported study was funded by RFBR, project number 19-37-90148.

References
[1] Guowang Miao, Jens Zander, Ki Won Sung and Ben Slimane 2016 Fundamentals of Mobile Data Networks (Cambridge University Press)
[2] What is DoS-attack? (Binance Academy) URL: https://www.binance.vision/ru/security/what-is-a-dos-attack
[3] Sharmila S and Umamaheswari G 2011 Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest AlgorithmsInternational Conference on Process Automation, Control and Computing (Coimbatore) pp 1–6
[4] Pandey, Rajshree 2014. Wormhole Attack in Wireless Sensor Network International Journal of Computer Networks and Communications Securityvol 2pp 22–26
[5] Monga H and Baghla S 2016 Approach to Security in Wireless Sensor Networks Applied Engineering Letters vol 1 no 3 pp 80–84
[6] Menezes A J Van Oorschot P C and Vanstone S A 1996 Handbook of Applied Cryptography (CRC Press)
[7] Zhang Y 2012 The Scheme of public key infrastructure for improving wireless sensor networks security Proceedings of IEEE 3rd International Conference pp 527-530
[8] Deny W D J Han Y S Chen S and Varshney P K 2004 A key management scheme for wireless sensor network using deployment knowledge
[9] Gungor O Chen F and Koksal C E 2015 Secrete key generation via localization and mobility IEEE Transactions on Vehicular Technology vol 6 pp 2214-2230
[10] Liu H Yang J Chen Y J and Koksal C E 2014 Group secret key generation via received signal strength: Protocols, achievable rates, and implementation IEEE Transactions on Mobile Computing vol 13 pp 2820-2835
[11] Wander A S Gura N Eberle H Gupta V and Shantz S C 2005 Energy analysis of public key cryptography for wireless sensor network 3 rd IEEE Conference on Pervasive Computing and Communications pp 324-328
[12] Amin F Jahangir A H and Rasifard H 2008 Analysis of Public-Key Cryptography for Wireless Sensor Networks Security International Journal of Information, Control and Computer Sciences vol 5
[13] Sedghi A K and Kaghazgaran M R 2013 Data Security via Public-Key Cryptography in Wireless Sensor Network International Journal on Cybernetics & Informatics vol 2 no 3
[14] Gabidulin E M 2013 Protection of information in telecommunication networksed E M Gabidulin, N I Pilipchuk, O V Trushina (Moscow: MITP- works vol 5 no 3).
[15] Paillier P 1999 Public-Key Cryptosystems Based on Composite Degree Residuosity Classes Advances in cryptology, EUROCRYPT’99 pp 223–238