ISSUES OF ENSURING INFORMATION SECURITY IN IOT SENSOR NETWORKS

Aliev Avazbek Ulugbek ugli
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan.

https://doi.org/10.5281/zenodo.19135935

Abstract. *The article examines issues of ensuring information security in IoT sensor networks. The structure of the security protocol is presented. Information is provided on methods to ensure the specific security of IoT sensor networks, such as secure node connection, protection from external influence, authentication and encryption for network layers, and registration for application layers.*

Keywords: *IoT sensor networks, IoT, data protection, security, confidentialit.*

In the world of machines and a highly automated society, IoT possesses immense power and influence. The issue of confidentiality and security for each individual within this society becomes an extremely complex problem to solve in practice, because the chain of security conditions created within its scope is virtually endless in content, and the weakest link determines the security level of the entire system. IPv6 has a sufficient number of IP addresses to cover the tens of billions of data points predicted to create our new world.

The issue lies in ensuring that all of them are protected to a degree that safeguards the individual's right to confidentiality and protects the system from malicious attacks. In conventional TCP/IP networks, the security system is created to protect the confidentiality, integrity, and availability of network data by ensuring protection of the system from malicious attacks that could lead to a loss of system reliability and cause denials of service and data disclosure.

Given the characteristics of node environments and application environments, the security of wireless sensor networks requires not only traditional security protection but also the existence of specific requirements regarding the protection, security, and confidentiality (TSP) of IoT sensor networks.

Protection, Security, and Confidentiality

Depending on the type of applications, IoT sensor networks may require TSP to ensure integrity, availability, confidentiality, non-repudiation, and user privacy. In IoT sensor networks TSP, it may be necessary to implement protection of nodes from unauthorized connection, and protection of communication channels and routing at the network layer may be required.

Registration/verification functions may be required to detect attacks on TSP.

IoT sensor networks TSP technology consists of message authentication, encryption, access control, authenticity identification, and others. The need for a TSP system in IoT sensor networks can be classified as follows: node security, cryptographic algorithms, key management, secure routing, data aggregation.

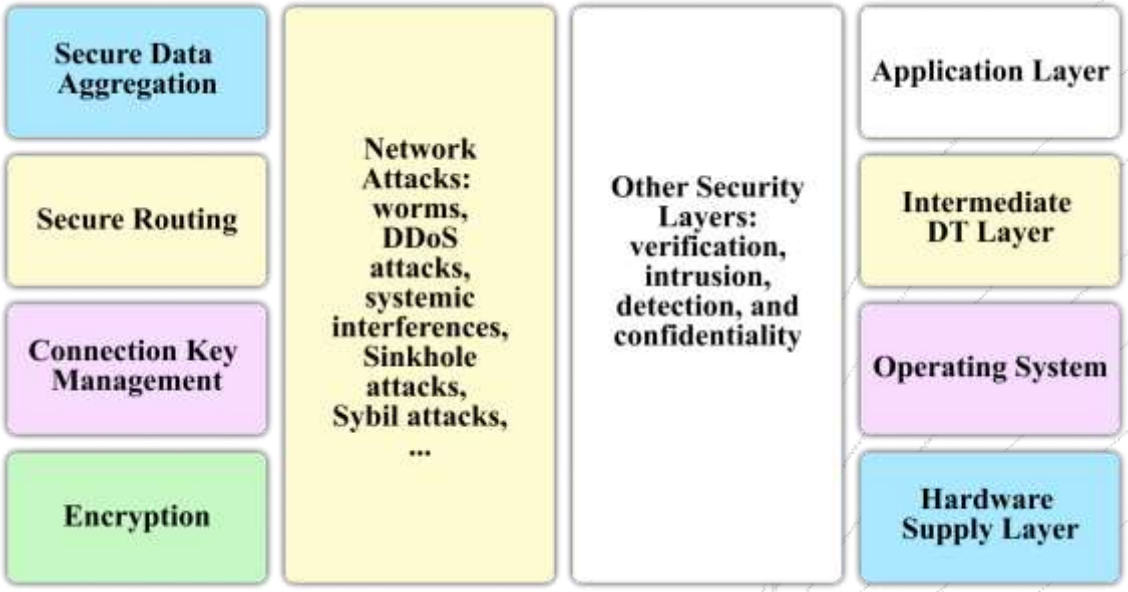

Figure 1. *TSP Architecture of IoT Sensor Networks*

Ensuring confidentiality, privacy as a human right, data security and integrity is very costly. The issue is: when considering the advantages offered by a solution, what will be the cost-benefit ratio? Must a person give up their rights to gain benefits?

Companies like Google and Apple have managed to obtain significant freedom in handling personal data for at least many users, where the benefit outweighs the risk. A public key infrastructure and a certifying company with authority within the scope of unlimited data sources will impose a tax on the system, and many players strive to minimize active security measures and resist only actually existing cyber attacks, thus endangering the entire system.

IoT networks that send malicious data packets to all connected systems are the very horror of any Hollywood film in the science fiction genre. Therefore, it is important for the maximum number of systems to operate independently of each other so that the vulnerability of one system does not harm the rest. Such a potential domino effect is considered the worst scenario, because poor data integrity can lead to unforeseen errors in some system. The effectiveness of active security systems will depend on understanding what the “normal” cyber-physical data flow is, but this could be an extremely expensive measure that reduces the benefits or increases the costs of IoT solutions.

Cryptographic Algorithms

Encryption is a special algorithm for altering the original data of a sensor node's data unit to prevent an unauthorized user from identifying the original data when accessing the encrypted data. Numerous operations are performed on wireless sensor networks within state infrastructure.

Traditional message authentication codes, symmetric encryption, and public-key encryption have shown many weaknesses. Therefore, a need has arisen for a new encryption system for IoT sensor networks.

The Spanish company Libelium developed the Waspmote encryption library in 2010 to ensure the security of smart city wireless sensor network data (Figure 2).

Essentially, their wireless sensor devices utilize these libraries. The libraries are intended for various encryption mechanisms and advisory mechanisms at the data transmission channel level, network level, and application level. In doing so, they extend it while ensuring the high security of the Zigbee® protocol.

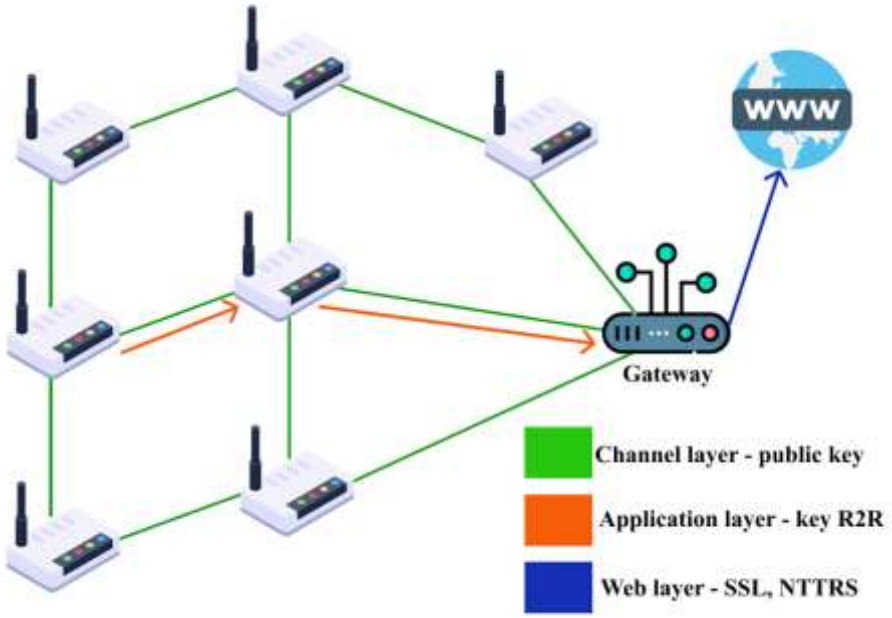

Figure 2. *Examples of using the Waspmote encryption library*

Key Management in IoT Sensor Networks

In general, a key management system is designed to ensure the security of wireless sensor networks. Key management includes key generation, distribution, verification, updating, storage, backup, ensuring validity, and destruction. An efficient key management system also serves as the basis for other security mechanisms such as secure routing, secure positioning, and data aggregation.

Common key management schemes in IoT sensor networks encompass general-use key management, random key management, location-based key management, cluster-based key management, and group-based key management. In the course of a secure initial boot procedure, a secure configuration of the sensor node is created, for example, a connection key is installed.

Consequently, there are many initial boot procedures, and choosing the appropriate procedure depends significantly on the specific environment. The normal operation of the sensor network is somewhat separated from the initial boot, meaning there is an opportunity to change the initial boot procedure without altering the security architecture for normal use. An appropriate initial boot procedure will depend significantly on the application and its environment.

Thus, several different initial boot procedures have been proposed:

- Hardware token;
- Pre-configuration of keys during node preparation;
- Physical protection of messages;
- In-band communication during a low-security configuration phase;
- Out-of-band communication.

Secure Routing in IoT Sensor Networks

Consequently, wireless sensor networks use several transit gateways and self-organization in the network for data transmission, requiring each node to also determine routing, establish routing, and service routing. A secure routing protocol is considered a fully efficient routing solution and may be a necessary condition for secure data aggregation and the secure loss of redundancy from the source node to the recipient node.

Many secure routed networks have been specifically developed for wireless sensor networks, which can be divided into three groups depending on the network structure:

- Linear routing;
- Hierarchical routing;
- Geographic routing.

Common methods of secure routing protocols include methods based on feedback data, location information, encryption algorithm-based methods, multi-channel selection, and hierarchical structure methods.

Various secure routing protocols can solve problems of different types of attacks. For example, there is a secure routing protocol based on feedback data containing information about delay, location protection, and excess power in the frame for verifying the medium access control (MAC) level connection. Within this method, although encryption is not used, it can provide protection against common attacks, such as false routing information, sinkhole, and worm attacks.

Many modern secure routing protocols assume the sensor network to be stationary, therefore there is a need to develop new secure routing protocols to ensure the mobility of sensor nodes.

Secure Data Aggregation in IoT Sensor Networks

Secure data aggregation is designed to ensure the security of each node. Thus, the general algorithm for secure data aggregation consists of the following. First, nodes provide reliable and accurate data and transmit it to large aggregator nodes. Large aggregator nodes check the accuracy of the data and perform calculations for aggregation based on redundancy.

Each aggregator node then selects the next secure and reliable transit gateway and transmits the data to the central node. The central node evaluates the accuracy of the data and performs the final aggregation calculations [4]. Initially, data aggregation was used to save energy, and security issues were almost not considered in its implementation.

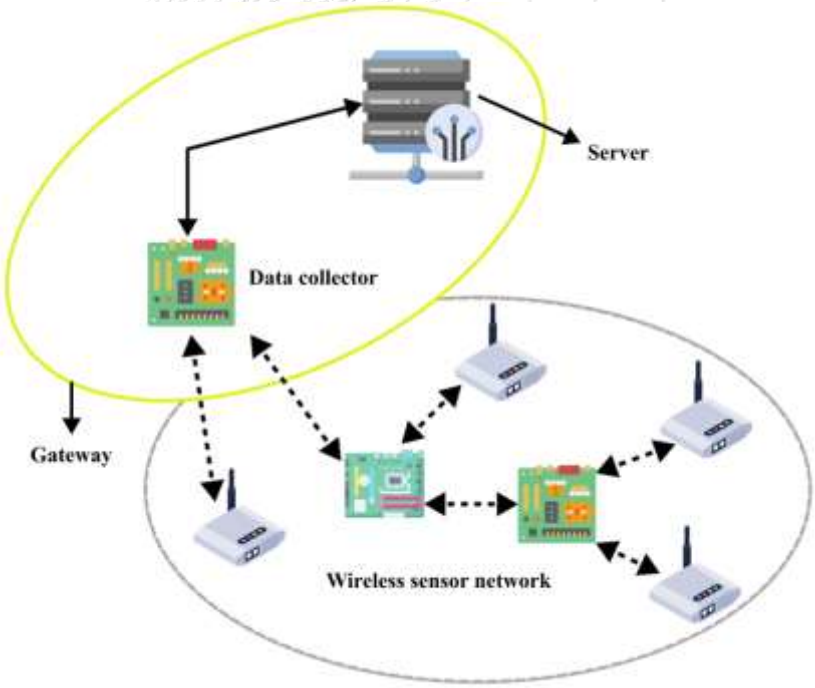

Figure 3. *Secure Data Aggregation*

Currently, secure data aggregation is mainly implemented based on cluster, ring, and hierarchy theory through authentication and encryption. The University of Munich created a data aggregation model based on the DTLS protocol for the practical implementation of secure transmission schemes. The blue circle in Figure 3 represents a model of secure data aggregation.

IoT Sensor Networks with Enhanced Security

Currently, IoT sensor network technology connects the infrastructure of organizations and enterprises with the information network. Damage caused to infrastructure (power supply system, transport system, chemical plant, and national security) through viral threats can lead to serious consequences.

IoT sensor networks are exposed to various security threats because an unmanaged transmission medium is more susceptible to attacks on the security system compared to a managed transmission medium. First and foremost, it is necessary to consider TSP (Protection, Security, and Confidentiality) issues. Threats faced by IoT sensor networks can be partially repelled with the help of network security technologies. The level of protection against complex attacks such as Sybil, DoS, and anomalous nodes is considered unsatisfactory.

The task of TSP regarding IoT sensor networks is to protect data and resources from attacks and illegal actions. Therefore, the criteria for achieving this goal are very broad and cover the following areas:

- Availability;
- Authorization;
- Authentication;
- Anonymity;
- Confidentiality;
- Timeliness;
- Integrity;
- Node protection;
- Non-repudiation;
- Privacy, etc.

In the future, the scale of IoT sensor networks may be significant, and the integration of IoT sensor networks with the Internet will become more organic. Despite significant research work in the fields of node security, encryption, key management, secure routing, and secure aggregation, serious measures need to be taken to ensure the security of IoT sensor networks in the future.

Structure of the Security Protocol

It is necessary to conduct research in the field of security protocol structure, which fits a general model for each IoT sensor network layer, taking into account computational capability, energy consumption, and the transmission capacity of the sensor node communication channel, as well as managing confidentiality and identification.

Consequently, a single solution in the field of one layer's security may not be the most effective solution; a holistic approach to ensuring security encompasses all common security layers in the network. Its objectives are aimed at increasing the efficiency of wireless sensor networks in terms of security, resilience, and connectivity.

The main principle is that the cost of security should not exceed a certain level of risk for security at a given time.

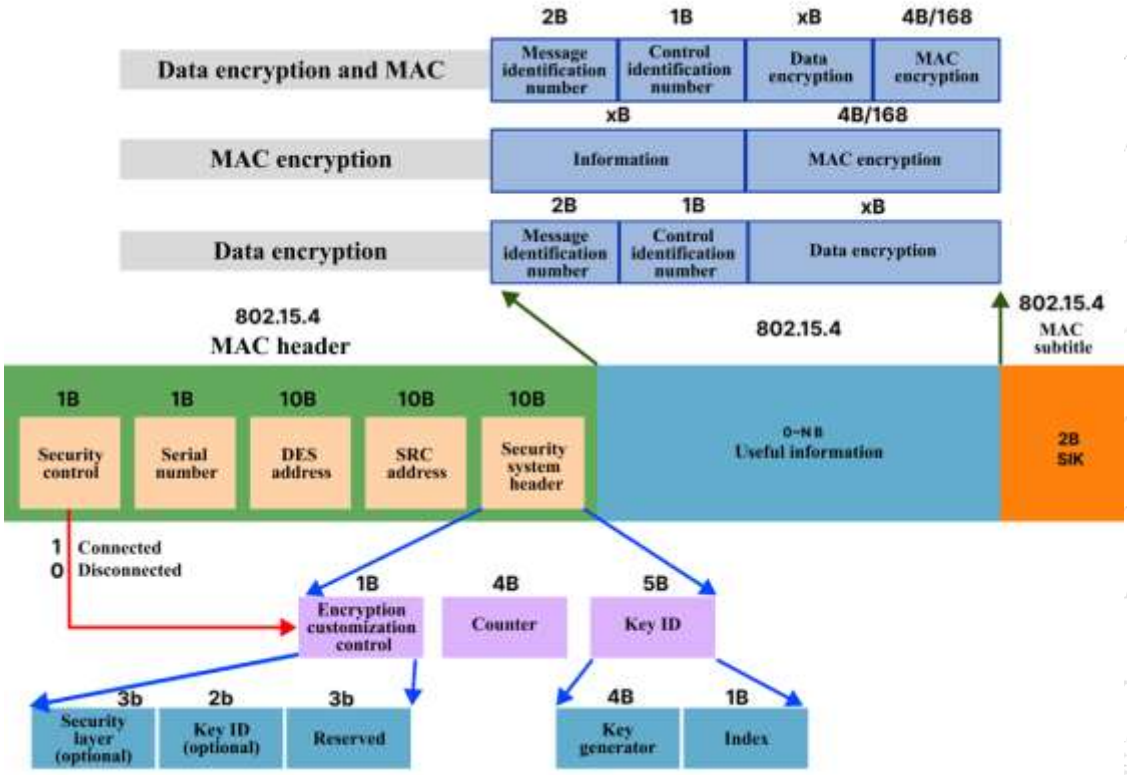

Figure 4. *Channel Layer of Security Protocol Structure*

Currently, there are many methods for ensuring the specific security of IoT sensor networks, such as secure node connection, protection from external influence, authentication and encryption for network layers, and registration for application layers.

At the same time, the order of structuring other layer protocols and creating the general infrastructure of the security protocol remains a serious problem for future research.

In the future, a general model will be created that can integrate all security layer mechanisms. Initial mechanisms will allow protecting IoT sensor networks from attacks, even if protection is bypassed to some degree.

At the same time, economic efficiency and energy efficiency may still be major problems to solve within the scope of research in the coming years.

For security purposes, the structure of IoT sensor networks will have four qualities (Figure 5). First, the security of IoT sensor networks is vulnerable to network attacks due to the nature of the broad data transmission medium and the limitations of sensor node computational resources such as low power and small transmission capacity.

Second, managing identification and protection is more complex and complicated in its meaning due to the deep integration of the information space with the physical world and connectivity to ubiquitous information technologies. Thus, managing the identification and protection system faces significant challenges.

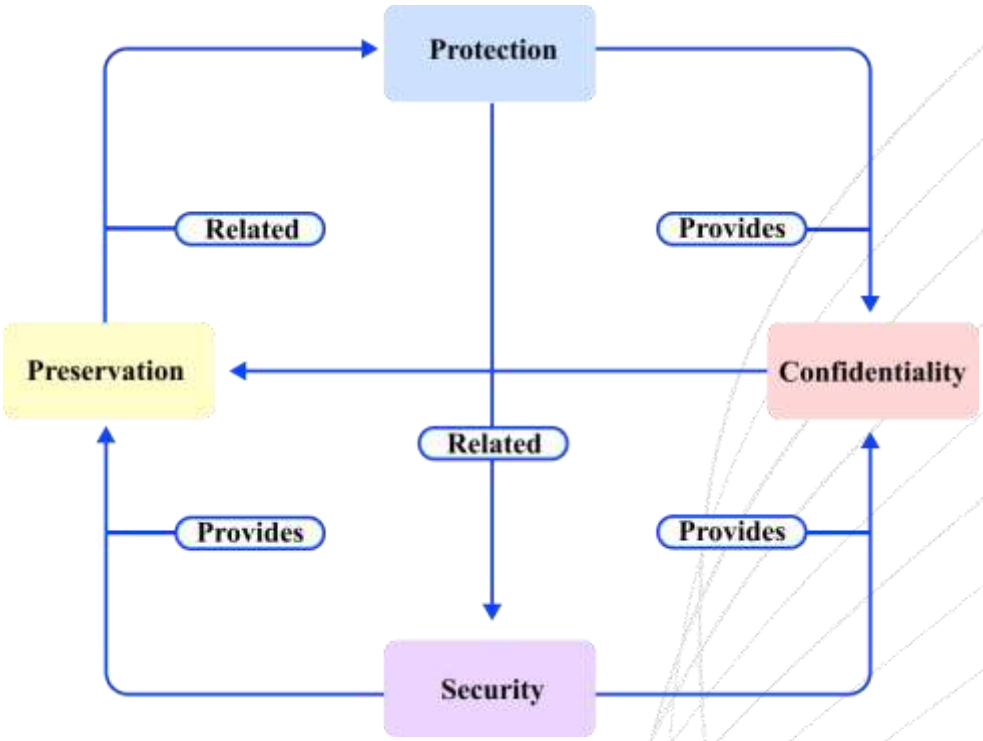

Figure 5. *Protection of Security and Confidentiality*

Third, the dynamic, heterogeneous, and massive characteristics of the reception and computational model of IoT sensor networks also pose serious problems for effectively protecting user privacy, such as system integrity, data integrity and confidentiality, identification, self-containment, and environment.

Finally, due to the large number of terminals, various types of terminals, and dynamic adaptive network structures in IoT sensor networks, the volume and complexity of environmental data pose serious problems for existing security control systems.

References

1. BLILAT, A., BOUAYAD, A., CHAOUI, N. and EL GHAZI, M. Wireless sensor network: Security challenges. Network Security and Systems (JNS2), 2017 National Days of. IEEE, 2017, pp. 6872. Available from: http://novintarjome.com/wp-content/uploads/2014/05/Wireless-Sensor-Network.pdf
2. LE X. H., SANK AR, R., KHALID, M., and SUNGYOUNG, L. Public key cryptography-based security scheme for wireless sensor networks in healthcare. Proceedings of the 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC '10). ACM, 2015.
3. KALITA, H. K. and K AR, A. Key management in secure self-organized wireless sensor network: a new approach. Proceedings of the International Conference and Workshop on Emerging Trends in Technology (ICWET '16). ACM, 2016, pp. 865870.
4. JHA, M. K. and SHARMA, T. P. Secure data aggregation in wireless sensor network: a survey. International Journal of Engineering Science and Technology (IJEST), Vol. 5, No. 3, 2016.
5. Rustam Maxamadov, & Mustafa Djamatov. (2025). Harbiy ta'lim muassasalarida mashg'ulotlarni tashkil etishda intellektual o‘qitish tizimlarining roli. «Muhandislik Va Iqtisodiyot» Jurnali, 3(9), 6–12. https://doi.org/10.5281/zenodo.17117077

6. Maxamadov Rustam Xabibullayevich, & Djamatov Mustafa Xatamovich. (2026). Technologies Of Artificial Intelligence in Optical Communication. Stanford Database Library of American Journal of Applied Science and Technology, 6(01), 27–31. Retrieved from https://oscarpubhouse.com/index.php/sdlajast/article/view/1022
7. Makhamadov Rustam Khabibullayevich, & Djamatov Mustafa Khatamovich. (2025). Modern intellectual systems: status, functions, technologies and development tendencies. American Journal Of Applied Science And Technology, 5(02), 52–55.
8. Mahamadov, R. (2022). Prospects for the application of artificial intellectual technologies in education. Technika [tecHnka], 1(7), 1-10.