The Authentication Method in Wireless Sensor Network Based on Neighbor Trust Model

Olesia Voitovych
dept. of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
voytovych.olesya@vntu.edu.ua

Olga Shulyatitska
dept. of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
olya_olek@ukr.net

Метод Автентифікації Сусідніх Вузлів в Сенсорній Мережі на Основі Моделі Довіри

Олеся Войтович
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
voytovych.olesya@vntu.edu.ua

Ольга Шулятицька
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
olya_olek@ukr.net

***Abstract* — Wireless sensor networks are rapidly developed and soon will occupy the dominant place among the other data collection and communication systems. The remote location of sensors and automatic operations within ones increase their vulnerability to external intrusions and attacks. Because of sensor supply necessity the authentication providing is quite challenging whereas the best protocols drain sensor capabilities. The method of sensor authentication within wireless sensor networks, which is based on the trust model, is proposed.**

Keywords — wireless sensor networks, sensor technology, authentication, trust model, energy consuming.

I. INTRODUCTION

Wireless sensor networks (WSN) increasingly penetrate the different fields of human activity. Sensor networks as part of the Internet of Things (IoT) occupy an important place in communication networks. However, research results show safety problems, those arise at the operation of these systems [1] including unsecured communication, weak authentication, lack of authorization, feasibility of used cryptographic algorithms, open libraries and updates exchange etc. Most of these problems are caused by such important feature of WSN as autonomic power supply, and those the duration of such a network performance is paramount.

WSN is a set of sensors, which are able to collect some data, transform it into electromagnetic signals, those are carried out by their broadcast, receiving signals from neighbor sensors and retransmit them on the air [2].

The wireless connection is easy enough for the intruder sensors packet interception. For example, most of the major threat is the denial of service attack, aimed to break the correct functioning of the sensor network. There are various options for anti-theft security systems, but most of them require substantial amount of resources, which is difficult to achieve at the strictly limited power supply conditions. Therefore, WSN requires new solutions for keys generation, their distribution, identification and protection [3].

II. THE WIRELESS SENSOR NETWORK ATTACKS

The problems of WSN information security can be divided into the primary and secondary issue. Primary targets are well known and cover confidentiality, integrity, availability and authentication of data. The secondary security issues cover data freshness, self-organizing, time synchronization, localization data [4].

A. Attacks on the WSN

The known attacks are shown in Fig. 1.

WSN are rapidly developing and soon will occupy a dominant place among the data collection and communication systems [3]. After analyzing the known attacks it can be concluded that to protect from the majority of attacks one needs to use authentication methods.

Classification features of sensor networks are proposed in [5]. One of the main features is power supply. WSN differ by power supply: self-powered (off-line), connected to the power supply (line) and renewable (energy that is collected from resources which are naturally replenished e.g. solar energy). This feature is very important because of WSN nature, which depends on battery or no, and thus can use more or less different processing resources.

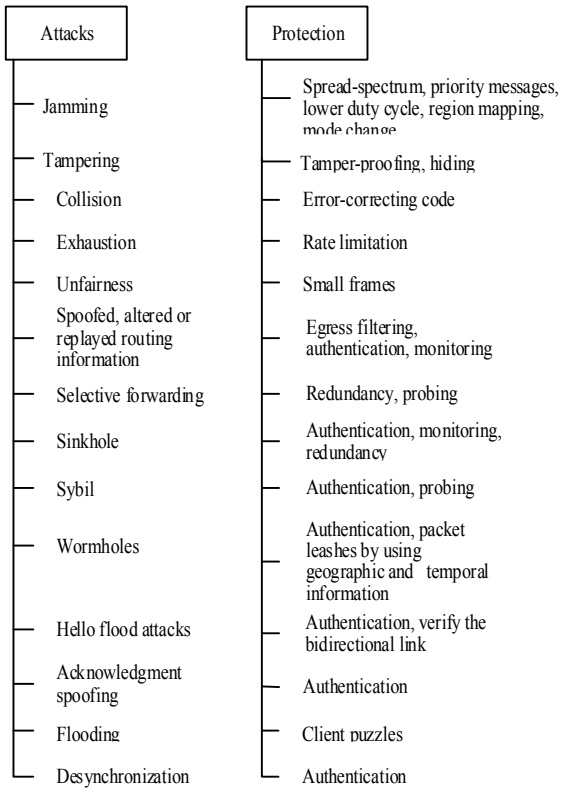

Fig. 1. Attacks on WSN and protection methods

III. The Authentication Methods Analizing

Today there are many authentications schemes in wireless sensor networks, the main ones are:

Based on the cryptography protocols, including lightweight protocols;

Based on hierarchies;

Based on the trust center.

For instance, in paper [6], author proposes a lightweight dynamic user authentication scheme that is built upon Wong et al. There is overall handshake in the scheme. The Wong's scheme consists of four phases: registration, login, authentication and password-changing phases. The first and the last phases are performed via a secure channel. There is a centralized gateway node in Wong's scheme and the performance in authentication process might be improved by designing a decentralized gateway node.

In paper [7], author proposes a broadcast authentication scheme for wireless sensor networks that utilizes a one-time signature scheme and re-keying mechanism. This scheme exhibits individual authentication, robustness to packet loss, and low overhead in computation, communication and storage. Author improves upon the one-time signature scheme, reducing the large key storage by using Merkle hash trees in generating the key pair. Despite increasing computation and communication efficiency, it significantly decreases the storage space usage [8].

In paper [9], the author proposes an enhanced Trust Center mechanism, which improves the performance of current standards in ZigBee Network with mobility node. In Trust Center, node of the initial authentication is achieved through the Trust Center. If the node will be moved to a different subnet, Trust Center shares authentication data with other Trust Centers without a separate authentication process. In order to evaluate the performance of the proposed scheme, the comparing of the energy and memory efficiency was performed.

There is a new authentication protocol in [10]. The trust center is not situated next to the joiner sensor. The master key is pre-shared between a trust center and a joined device, and the network key is distributed to every parent router in the network by the trust center, the same way as at authentication protocol within ZigBee. In addition, the local authentication key, which is used in pre-authentication procedure, is pre-shared between a parent router and the joiner device to be used in pre-authentication procedure.

In [11], author describes communications model and trust model, considering the scenario where a mobile user, associated with its home agent, is visiting a foreign network with a foreign agent. When mobile user is out of its home network, it needs to be authenticated before being allowed to access a visited foreign network. Because mobile user is out of the coverage of its home agent, author assumes that any message between mobile user and home agent has to go through foreign agent. Author further assumes that home agent has a communication link to the foreign agent that is to serve mobile user. A secure channel can be established between home agent and foreign agent, for example, via Kerberos [12].

Fig. 2 shows the trust model, where a dashed line with arrows at both ends indicates that there is mutual trust established between the two end parties, and a dashed line with an arrow at one end only indicates a one-way trust. Following Fig. 2, mobile user cannot trust foreign agent and vice versa, when MU – mobile user, HA – home agent, FA – foreign agent, AS - authentication server.

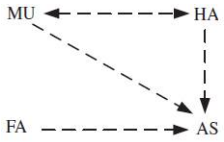

Fig. 2. Trust model accordig to [12]

Typically, there is no bilateral trust between foreign agent and home agent. Although mobile user trusts, authentication server and home agent in case of direct communication absence in foreign network, the proper authentication is to be used. All other trusting pairs connected via dashed lines in Fig. 2 are straightforward to follow.

Thus, the lack of these authentication methods has three problems:

Weak methods are easy to break, as a result of the traffic analyses, data modifying, the sensor substitution etc.

Cryptography methods need too large energy consumption, which is bad from the practical point of view. Using

complex cryptographic authentication scheme consumes a lot of energy for data transmission and processing as a result sensor battery needs charging or replacing, so this issue is relevant for the decision.

Additional trust centers reduce flexibility of WSN and can be victim of attackers.

IV. Proposed Authentication Methods Based on Trust Model

The authentication method based on trust model with a poll of at least three neighbor nodes, which solves the above-mentioned problems, is proposed. At the energy-efficient routing protocols [13-18], the sensor asks neighbors about their readiness for data transferring (level of battery, distance from each other etc) to construct the optimal data transfer route. That is why it is proposed to request additional options (level of trust) during this data exchange. Fig. 3 schematically shows the idea of authentication process performance (ID – Identifier, K – Key, RD - Level of trust (1 or 0), SN - Node (sensor), Bat – Power, Route - Remoteness).

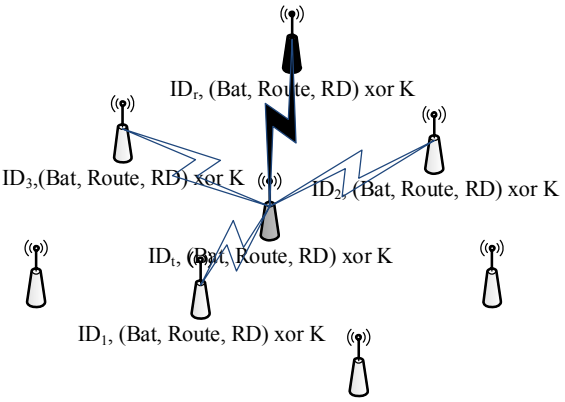

Fig. 3. Transfer data scheme of the WSN (gray - transmitter, black - receiver)

Let's assume there is a sensor network and each sensor (node) has a small database, that contains minimum of three neighbor nodes IDs to further authenticate and determine the level of trust in other nodes. This authentication scheme is a simple request-response protocol, which involves such components: transmitter node (SN_t), receiver node (SN_r) and respond nodes (SN_i). The transmitter node (SN_t), which is to send data firstly requests at least three trusted sensor nodes whether or not the receiver node (SN_r) is trusted by them. Moreover, if the nodes majority answers positively, the receiver node would become trusted. Thus, transmitter node forms an overall picture either transmits data or polls other nodes and searches another route.

1) *Registration phase*

At the registration phase more complex authentication schemes could be used bearing in mind above statements for nodes in WSN. They provide greater stability because of the more complicated authentication usage. Neighbor nodes participating in the scheme and authentication need only to perform authentication three times and new node would be considered as trusted one.

Once the node successfully completes the registration phase for three nearest nodes, it becomes trusted. Since such authentication requires a small number of iterations (only for neighbor nodes) this would save energy supply. As a key for further sharing can be used mentioned battery level. The battery charge value can be used to avoid pseudo-random numbers generation. The value of the battery charge is a true random number after trend elimination (e.g. Bat = 78,854, then ID is 854).

2) *Authentication phase*

Case 1: neighbor sensors are trusted. Transmitter node (SN_t) polls the neighbor sensors about their resources level (Battery) and the routing data (Route); as a result the optimal energy-efficient route is received. As the polled neighbor sensors (SN_1, SN_2, SN_3) are trusted and have the shared key (K) (received at the registration phase) the information is to be transmitted.

Case 2: new neighbor sensor is appeared. When the new sensor (SNr) tries to take part at the communication, it must pass a strong authentication during registration phase to receive a shared key.

Step 1: transmitter node (SN_t) forms the request, which contains the following parameters: identifier ID_t, key (K) (the shared key can be formed from energy values, without trend, and therefore does not require additional resources for its generation), energy level (Battery) and routing data (Route), and requests for the same settings from its neighbor nodes. The request includes the trust level (RD) too. The transmitter node (SN_t) wants to know whether or not receiver node (SN_r) is trusted. Moreover, all data transmitted and accepted to be encrypted using XOR on key (K) that obtained during registration phase.

Step 2: at this step transmitter gets the response from the nodes SN1, SN2, SN3, which contains IDs, energy levels (Battery), routing data (Route) and trust level of the receiver node SN_r and the most importantly his personal ID (the battery without trend obtained at the registration phase).

After these steps transmitter node (SN_t) forms the decision concerning data transfer to receiver node (SN_r). The transmitter node determines the optimal route based on the data, that is received from neighbor nodes. Using the level of supply and optimal route distance the optimal route is formed, and using level of trust transmitter node makes the decision concerning data transferring.

The proposed WSN was simulated using environment Atarraya. Modeling was performed by Atarraya emulator [19] - the simulator control events that could be used for teaching and researching of management protocols and wireless network topology. It is designed to be run on Windows platform. The simulator consists of two topologies: TC - Topology Constructions; TM - Topology Maintenance. Two protocols are selected: DGETRec - each time, that node reaches a critical energy threshold, the topology maintenance algorithm terminates the previous reduced topology and invokes the topology construction algorithm to create a new one [20]; DLEDSR - each time, that node reaches a critical

energy threshold, the local topology maintenance algorithm based on the DSR protocol repairs the topology [20].

The experiment showed (fig.4) the implementation of different energy efficient protocols, but with identical parameters such as the number of nodes (100 nodes), the same amount of transmitted data and the same weight of this information etc. Comparison of results is rather impressive. In the first case of EECDS protocol using WSN was almost not working, nodes lost their charge and couldn't transmit data, in other case of Energy Local Patching DSR protocol using network was fully functioning when nodes have high battery power they were able continue their work even greater amount of time, unlike the first case.

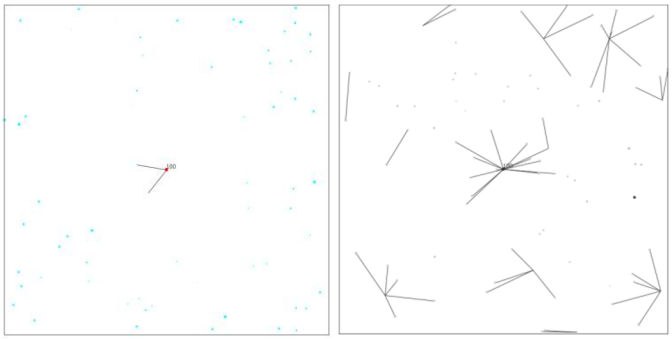

Fig. 4. WSN modeling (1. TC – EECDS, TM – DGETRec time work network = 3000012.345; 2. TC – EECDS, TM – Energy Local Patching DSR time work network = 3000000.3)

So the extension of power supply for each unit was gained, and thus the duration of the service provided by the network was increased for quite much time. It would provide decreasing of network maintenance, consequently the network would be more economical.

V. CONCLUSION

Since WSN found the widespread usage at the Internet of Things, which development is very fast-paced, there are two major problems: security of data transmitted and fast unit (with battery) power reduction. This article was aimed at addressing these two issues. The primary and secondary security issues as well as the real attacks on wireless sensor networks were analyzed. Based on main attacks and protection mechanism the problem of authentication in wireless sensor network is allocated. The existing authentication schemes often drain very much battery energy and cannot be used widely.

The method of authentication in WSN, which provides a stable authentication using the minimum amount of resources, was proposed. The authentication method is based on the trust model, that considers usage of a complex authentication only at the registration phase and provides network protection by doing this. Using neighbor trust model for simplifying authentication during other communications provide power consuming decreasing of the WSN. The experiment proved that the usage of protocols increases efficient supply network lifetime, therefore reducing network maintenance costs.

REFERENCES

[1] Operating problems WSN: http://blog.ioactive.com /2017/02/hacking-robots-before-skynet.html

[2] S. Yinbiao, P. Lanctot, F. Jianbin, “Internet of things: wireless sensor networks,” White Paper, International Electrotechnical Commission, 2014.

[3] A. Roslyakov, S. Vanyashin , A. Scallops, M. Samsonov, “Internet of Things,” Samara, 2014 (in Russion).

[4] G. J. Fan, S. Y. Jin, “Coverage problem in wireless sensor network: A survey,” Journal of Networks, vol. 5, №. 9, pp. 1033-1040, 2010.

[5] O.Voitovych, O.Shulyatitska, V.Malyushytskyy, Simulation and security of sensor networks: Inżynier XXI wieku projectujemy przyszlosc, monografia [pod red: Jacek Rysiński] - Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016 – pp. 367-373. ISBN: 978-83-65182-51-7.

[6] H. R. Tseng, R. H. Jan, W. Yang, “An improved dynamic user authentication scheme for wireless sensor networks,” Global Telecommunications Conference, pp. 986-990, 2007.

[7] S. M. Chang, et al., “An efficient broadcast authentication scheme in wireless sensor networks,” Proceedings of the 2006 ACM Symposium on Information, computer and communications security, ACM, pp. 311-320, 2006.

[8] Volodymyr Luzhetsky, Yurii Baryshev. Methods of Generic Attacks Infeasibility Increasing for Hash Functions // The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS’2013), September 12-14, 2013 Berlin, Germany. Available: idaacs.net/2013/wp-content/uploads/abstracts/i13-071_8d0bb875.rtf

[9] K. Lee, et al., “An enhanced Trust Center based authentication in ZigBee networks,” International Conference on Information Security and Assurance, Springer Berlin Heidelberg, pp. 471-484, 2009.

[10] S. H. Lee, J. H. Kim, “Design of authentication protocol for LR-WPAN using pre-authentication mechanism,” Consumer Communications and Networking Conference, pp. 1-5, 2009.

[11] C. Chen, et al., “Lightweight and provably secure user authentication with anonymity for the global mobility network,” International Journal of Communication Systems, vol. 24, №. 3, pp. 347-362, 2011.

[12] B. C. Neuman, Ts'o T. Kerberos, “An authentication service for computer networks,” IEEE Communications magazine, vol. 32, №. 9, pp. 33-38, 1994.

[13] V. Karthikeyan, A. Vinod, P. Jeyakumar, “An Energy Efficient Neighbour Node Discovery Method for Wireless Sensor Networks,” 2014.

[14] Y. Chung, “An energy-efficient unicast routing protocol for wireless sensor Networks,” Tech. Int. J. Comput. Sci. Emerg. Tech. – 2011. – vol. 2. – pp. 60-64.

[15] R. Tiwari, A. Saxena, “A review on energy efficient routing in wireless sensor networks,” Journal of engineering trends and technology, 2015. Vol 19. pp. 29-34.

[16] A. G. A. Elrahim, et al., “An energy aware WSN geographic routing protocol,” Universal Journal of Computer Science and Engineering Technology, 2010. – vol. 1. pp. 105-111.

[17] G. Krishna Priya, Dr. G. Prakash Babu, “EE-DSR: Energy Efficient Dynamic Source Routing in Wireless Ad Hoc Networks Using Residual Energy,” International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, 2015 pp. 134-138.

[18] R. Alasem, A. Reda, M. Mansour, “Location based energy-efficient reliable routing protocol for wireless sensor networks,” Recent Researches in Communications, Automation, Signal processing, Nanotechnology, Astronomy and Nuclear Physics, WSEAS Press, Cambridge, UK, 2011 pp. 180-185.

[19] Simulation Atarraya. Available: http://www.csee.usf.edu/~mlabrador/Atarraya/

[20] P. M. Wightman Rojas, Topology control in wireless sensor networks. – 2010.