Modelling attacks in self-organizing wireless sensor networks of smart cities

A V Meleshko, V A Desnitsky* and I V Kotenko

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 199178, 39, 14-th Linia, St. Petersburg, Russia

*desnitsky@comsec.spb.ru

Abstract. Nowadays self-organizing wireless sensor networks for solving the problems of arranging operational processes in smart city systems are becoming rapidly developed and widespread. Such networks are used to collect and aggregate data from physical sensors of devices as well as for its processing and transmission over the network in conditions of time-varying loading characteristics of the communication channels, changing location of devices and their operating modes. The paper discloses an approach to modeling and analysis of attacks aimed at compromising devices, data and services of smart city systems built on the basis of self-organizing wireless sensor networks.

1. Introduction

Using of wireless sensor networks (WSN) in various application fields, including for the implementation of Digital City systems, is becoming increasingly widespread. Moreover in case of using WSN within a critical infrastructure, an increased attention should be paid to security of such networks [1]. Self-organization possibilities of such networks impose additional risks associated with the unauthorized use and modification of the network and its services by both external and internal information security intruders. Attacks aimed at the industrial cyber-physical systems of the Digital City, if successful, can lead to serious and even catastrophic consequences of anthropogenic and social nature, as well as to significant financial damage. To prevent deliberate negative effects and reduce possible damage from them, an approach to modeling attacks on Digital City systems is proposed. The modeling is performed for research purposes in laboratory conditions in order to identify core features of such attacks and the conditions for their implementation.

The main contribution of the paper lies in, first, the constructed model of attacks on the WSN nodes of Digital City systems, having identified five types of attacks that exploit properties of WSN self-organization, and, second, the approach to model attacks on self-organizing WSN. The distinctive feature of this approach is its combined nature, including methods of analytical, natural and simulation modeling. The proposed approach has been tested on a fragment of a prototype of a cyber-physical system for monitoring the state of atmospheric air. It is built on the basis of communication modules Digi XBee s2. Experiments on modeling of the attacks examined in the work have confirmed the validity of the approach.

The rest of the paper is organized as follows. Section 2 provides an overview of the related work in the field. Section 3 presents a general model of possible attacks exploiting self-organization of WSN.
Section 4 reveals the essence of the proposed approach to attack modeling. Section 5 discloses the analysis of results and discussion. The last section concludes the paper.

2. Related work

A number of existing papers [2-5] are devoted to research into specific security issues and attacks on wireless sensor networks in various problem domains. Particularly in [5], Khan and Khan highlight the basic requirements aimed at ensuring WSN security, including ones for confidentiality of transmitted data, their integrity and availability of network nodes and non-repudiation of actor's actions. To achieve these requirements, it is necessary to make efforts to counter possible malicious effects, which are advisable to apply, taking into account characteristics of the expected types of attacks as well as structure and functional features of the target system.

A network should be resistant to attacks, since attacks can lead to distortion of information and as a result to the adoption of the wrong business decisions. In [6] Grover and Sharma study various security issues and security threats in the WSN. A brief description of some of the protocols used to achieve network security is also provided. The following relevant types of attacks are disclosed in [6]: Wormhole, HelloFlood, Selective attacks, Sybil attacks, Sinkhole, performed by an intruder at physical, channel, transport, and network interaction levels and required to apply specific modeling means to ensure security.

Vikhyath and Brahmanand discuss particular problems that can be encountered while ensuring security of the WSN, including limited resources of WSN nodes, limited power and memory [7]. Having limited resources it is needed to concentrate on reliability of data transmission, data freshness, node authentication, confidentiality, integrity. Vikhyath and Brahmanand also describe specific attacks at various levels of the WSN, and a table with a description of countermeasures to prevent such attacks is presented. For example, at the physical level, they single out attacks like interference, eavesdropping, device hacking. At the data link layer it includes violation of synchronization of packet sending time. Attacks at the network level are false routing and replaying of packets.

Note that despite the fact that WSN security as well as both general and private approaches to its organization are adequately covered in the existing scientific and technical literature, the security issues of self-organizing WSN, and in particular attacks exploiting the self-organizing property of a network, deserve additional attention of researchers. As promising tools and environments for modeling attacks on WSN, which are appropriate for evaluating and comparing various types of attacks, one may include software tools for mathematical and program modeling of networks, including ones based on state transition schemes and other approaches to verification of technical systems.

3. Attack model

To ensure security of contemporary cyber-physical systems and networks operating within the Digital City infrastructure, it is advisable, first, to analyze possible and most critical attack effects and, second, to evaluate organizational and technical complexity of the attack, its criticality and practical feasibility as well as to identify ways to increase security of the infrastructure. Evaluation of attacks is performed by using various modeling methods. Given the specificity of Digital City systems, including heterogeneous and interconnected mobile, moving in space and stationary technical facilities and infrastructure elements, attacks exploiting self-organization properties of the wireless communication sensor network of a Digital City system deserve an increased attention.

The proposed attack model is based on two existing classifications of intruders of the cyber-physical devices, namely according to the level of capabilities of the intruder [8] and by the type of access to the attacked device [9]. In particular, one can distinguish three levels of the intruder's capabilities: (1) exploitation of known vulnerabilities and the use of publicly available software tools, (2) ability to develop and adapt specialized software and hardware tools, (3) unlimited organizational and technical and financial resources the attacker owns [8]. The following five types of intruder access to an attacked device are defined in [9]: (1) manipulating the device using social engineering methods,
Having a certain level of capabilities and type of access to WSN nodes, an intruder is able to perform attacks related to modifications of sensors, tamper with methods of processing data from them, illegitimate connection and use of communication interfaces of network nodes, installation of malicious software on the central control node, modification of firmware of microcontrollers of nodes and other factors in the functioning of the network. Within the framework of the proposed attack model, we distinguish five main types of attacking influences on the wireless sensor network on the base of the illegitimate use of the WSN self-organization in order to violate the integrity, confidentiality and availability of network nodes, data and provided services (Table 1).

Table 1. Types of attacks on WSN through the use of its self-organization functionality.

| Attack type | The exploited functionality of the self-organizing network | Attack description |
|-------------|----------------------------------------------------------|--------------------|
| Type 1      | Functions of dynamic network rebuilding to optimize its functional and non-functional characteristics (including for balancing the load of communication channels) | Man-in-the-Middle attack, which includes penetration of a false or compromised node into the network and the passage of all or part of the data flows through this node. The attacker is able to listen and modify the transmitted data, send service commands for illegitimate rebuilding of the network |
| Type 2      | Functions of temporarily disconnecting a node to ensure rebuilding the network topology | Man-in-the-End attack on WSN node with the ability to replace/modify its firmware |
| Type 3      | Functions of dynamic rebuilding a network topology with a change in time of the set of the WSN nodes | An attack of an illegitimate violation of network connectivity, in particular, forced shutdown of a network node by an attacker under the guise of a legitimate network modification |
| Type 4      | Dynamic rebuilding of network topology with changing methods and routes of network connections | The attack represents malicious influence on nodes that have elevated privileges and access rights to the network data and network services with the aim of manipulating this data and illegitimate use of the services |
| Type 5      | Cooperative services for the use and management of WSN and group based decision-making for network nodes | The attack represents an impact on a group of WSN nodes to unreasonably take a group based decision on the structural and functional modification of the network or perform some agreed actions by them |

In particular, by performing a Type 1 attack, an intruder can divide the network into two or more disjoint segments, all communications between which are controlled by the intruder. For a Type 5 attack, depending on the control and decision-making rules in the network, malicious influence can be initiated merely by minimal intruder's manipulation on the parameters of the network or physical environment. In addition, a Type 5 attack may represent deployment of a botnet within the framework of the WSN. Specifically it can assume excessive generation of traffic exploiting self-organizing functions. This can lead to DDoS attacks, which purpose could be either internal network nodes or external network devices.

Based on the constructed attack model we are using the following analytical approach to verify the presentation model of a specific WSN. By combining the both classifications [8-9], a matrix of 15 categories of the intruder is built. Each category is expertly compared with the specification of the modeled WSN in order to identify the relevant categories of the intruder, which it is worth to protect the network against with the subsequent formation of appropriate countermeasures.
4. Combined approach to simulate attacks against self-organizing WSN

For a comprehensive evaluation of the investigated types of attacks on self-organizing wireless sensor networks, specific methods of modeling the attacks on WSN are used. The proposed combined attack modeling approach includes:

– methods of analytical modeling, allowing on the basis of existing models and classifications of an intruder to determine analytically the most critical types of attacks that the WSN is subject to, including taking into account the risks of compromising the network and the value of its assets;

– imitation modeling (i.e. simulation) methods used on the basis of specialized software simulators, such as NetSim, OMNeT ++, NS-2, NS-3 and J-Sim used in conditions of the absence or insufficiently presence of the hardware required for other types of modeling;

– methods of natural (or physical) modeling, which attacks effects are modeled on a physical hardware-software prototype of a WSN in, including by using of ZigBee, SigFox, LoRaWAN hardware platforms and protocols.

Let us regard advantages and limitations of each of the used modeling methods. A natural WSN model is the one closest to the conditions of a real WSN in terms of the possibility of using industrial instances of network nodes operating in conditions close to the real functioning conditions. At the same time, the disadvantages of natural modeling assume the organizational and technical complexity of forming such models of large-scale networks, as well as launching complex multi-step attack scenarios on it for the research purposes, involving a large number of nodes. The disadvantages of natural modeling include also the limited resources of the network with its current values, the difficulty of modifying the parameters of the software and hardware environment of the network, the need to manually adjust each node, the presence of possible failures and hard to catch errors at the crossing of the software and hardware levels of network representation, as well as the potentially high cost of buying new and maintaining the physical equipment.

The advantages of the imitating modeling include the ability to simulate a network at a certain level of abstraction without being tied to a specific hardware platform of the network, the ability to dynamically tuning the network as a whole and its individual nodes on the fly. It could be done both in terms of changing the quantity of nodes and hardware and software characteristics of the resources available to them. Also the simulation provides an ability to design complex multi-step resource-consuming network scenarios based on dynamically configured patterns of node behavior. The deployment of a network model can be performed quickly and by using automation tools as well. The main disadvantages of WSN simulation models include the need to prove the correctness and consistency of such models, as well as check its structural-functional and behavioral correspondence to the instances of real networks.

The distinctive features of WSN analytical models include the possibility to draw conclusions about the potential exposure of network nodes to certain types of attacks, having merely minimal data on the WSN. In addition, such modeling can be performed at the earliest stages of the WSN design process, even having no physical equipment yet. The disadvantages of such models include the potentially high complexity of predicting resource consumption and other operational non-functional characteristics in the modeled network processes.

Within the context task of modeling attacks in self-organizing WSN, the natural modeling is used to examine attacks on a laboratory WSN software/hardware prototype, which operates in some modeled conditions with certain assumptions. In our work, first of all this type of modeling is used to investigate attacks of types 1-4. At the same time we are using imitation modeling to simulate attacks of type 5, where it is required to model more complex interaction logic between groups of nodes, including longer interaction. Analytical modeling is used for all types of malicious effects to establish the most relevant types of attacks the conditions of their occurrence.

Figure 1 schematically shows a generalized technique for applying a combined approach to modeling attacks on a WSN. The input data are the specification of a specific system and existing knowledge models about attacks on cyber-physical devices. At the stage of analytical modeling for a specific Digital City system, we determine the relevant types of attacks which the nodes of the
underlying WSN are exposed to. In particular, attacks are ranked by the degree of their criticality and the difficulty of their performance by a potential attacker. Further, the selected attacks are modeled on a natural test-bench, as well as by using simulation tools. Furthermore, for each type of attack the choice of the modeling tool is conducted individually, depending on the nature of the attack and the conditions of its feasibility.

The output of the technique is results of the assessment of the modeled attacks. This outcome is, expressed in form of values of the target security indicators of the system, its devices, data and services provided as well as indicators of the organizational and technical complexity of attacks, including numerical indicators of the duration of the attack and the number of compromised network nodes involved. The attacks of all five types presented in the framework of the attack model were modeled analytically. Type 1-4 attacks are modeled on a natural test-bench, while Type 5 attacks are modeled by means of simulation.

As a practical part of the work, instances of Type 1-4 attacks were modeled on a physical prototype of the Digital City system built on the basis of a wireless sensor network by using XBee s2 wireless communication modules, Arduino Mega 2560 microcontrollers and a number of sensors of physical environment characteristics. As an illustration, a fragment of the hardware/software prototype of the Digital City system for monitoring the characteristics of air pollution without attack and with a modulated attack of type 1 are shown schematically in Fig. 2 and 3, respectively.

![Figure 1. Combined technique for modeling of attacks on WSN.](image1)

![Figure 2. A fragment of a prototype of a wireless sensor network for Smart City.](image2)
Figure 3. A fragment of a prototype of a wireless sensor network for Smart City with a modeled attack of type 1.

Communications within the laboratory prototype of the wireless sensor network are performed in compliance of ZigBee protocol. Figure 2 shows the legitimate modules of the Digi XBee s2 based network, which collect data from sensors and send them to the control server for processing them by using dynamically selected routes. In Figure 3 the scenario of the intruder’s actions includes penetration of an attacking XBee module and its physical situation between two groups of nodes to perform a Man-in-the-Middle attack. Such an attack includes listening, intercepting and replacing of sensors readings and service commands transmitted over the network. After being penetrated into the network, the attacker sends commands to the neighboring nodes to force the signal to decrease their power level in order to redirect all the communication channels between the two groups of nodes to itself.

A variation of this attack as a result of a forced decrease of the power of the attacked network nodes may be also a breakdown in the network connectivity. At that such breakdown elimination may require manual manipulation of each of the attacked modules. As a result the network’s operability and the trustworthiness of the data being collected can be compromised for a long time [10].

The modeled Type 5 attack represents a distributed energy depletion attack performed by a group of compromised nodes and is targeted on a mobile device operating autonomously by using exhaustible energy source. In our work this attack is modeled by means of J-SIM simulation environment.

5. Discussion and evaluation of the results

The conducted experiments on modeling attacks of types 1-5 showed feasibility and validity of the proposed combined approach to modeling self-organizing WSNs. The experiments allowed us to make use of evaluation of feasibility of attacks and determine the basic conditions and key characteristics of attacks for the subsequent construction of measures to counter these attacks. Feasibility of the examined attacks of types 1-5 is reduced to a presence of the network self-organization properties to be exploited by an intruder. At the same time, we note that the choice of a particular modeling environment directly depends on the conditions of the attack. The choice of modeling tools should be
made individually for each type of attacks, taking into account the size and variety of assets of the system in question.

Based on a prototype of a wireless sensor network available in the laboratory, the natural modeling on a software/hardware prototype allowed simulating simplified varieties of the attacks to obtain their rapid estimates. After obtaining these express estimates their further modeling is possible by using simulation tools that provide network scaling and eliminating resource and technological limitations imposed by a particular hardware platform. In particular, the use of simulation tools seems appropriate for the study of a wide class of attacks, including flood attacks, network scanning of WSN nodes, distributed denial of service attacks and Denial-of-Sleep attacks.

The proposed combined approach to modeling attacks on self-organizing WSN is also reasonable to use in order to develop countermeasures, both in terms of preventing attacks based on refinement of WSN architectural solutions and in terms of responding to identified security incidents. The reactions include, in particular, notifying of the operator on a detected security incident, blocking the operation of nodes considered as attackers, filtering a certain type of data packet in the network and intentionally reducing the throughput of some communication channels. The results of the proposed modeling approach are supposed to be used primarily to develop countermeasures for the most significant attacks in various fields of application of Digital City systems. Attacks that use the features of the interaction of groups of interconnected and moving in space nodes that provide certain services, such as control systems for unmanned vehicles are of a particular interest.

6. Conclusion

The paper proposed an approach to modeling attacks in wireless sensor networks on example of a Digital City system. The distinguishing features of the approach lies in its combined nature, including three types of modeling - analytical, natural and simulation modeling, as well as in its focus on malicious effects that exploit properties of the network self-organization. The approach was tested on the hardware/software prototype of the Digital City system, and the feasibility of attacks exploiting the network self-organization has been shown. As a part of further research, it is planned to examine countermeasures to the regarded types of attacks, including those ones performed at the design stage of such systems.

Acknowledgments
This work was partially supported by a grant of RFBR (19-07-00953) and by the budget project 0073-2019-0002.

References
[1] Desnitsky V., Chechulin A., Kotenko I., Levshun D., Kolomeec M. 2016 Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System SPIIRAS Proceedings issue 48 pp 5-31.
[2] Bangash Y.A., Abid Q.D., Abed Ali A., Yahya E. A. 2017 Security Issues and Challenges in Wireless Sensor Networks: A Survey International Journal of Computer Science no 44:2 pp 1-15.
[3] Yang G., Dai L., Wei Z. 2018 Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks Sensors vol 18 no 3907 pp 1-26.
[4] Yanga G., Daia L., Sia G., Wanga S., Wanga S. 2019 Challenges and Security Issues in Underwater Wireless Sensor Networks Procedia Computer Science vol 147 pp 210-216.
[5] Khan M.A., Khan M. 2019 A Review on Security Attacks and Solution in Wireless Sensor Networks American Journal of Computer Science and Information Technology vol 7 no 1:31 pp 1-7.
[6] Grover J., Sharma S. 2016 Security Issues in Wireless Sensor Network – A Review 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and FutureDirections) pp 397-404.
[7] Vikhyath K.B, Dr. Brahmanand S.H. 2018 *Wireless sensor networks security issues and challenges: A survey* International Journal of Engineering & Technology vol 7 pp 89-94.

[8] Abraham D., Dolan G., Double G., Stevens G. 1991 *Transaction security system* IBM Systems Journal vol 30 no 2 pp.206-228.

[9] Rae A. Wildman L. 2003 *A Taxonomy of Attacks on Secure Devices* Australian Information Warfare and IT Security pp.251-264.

[10] Desnitsky V., Kotenko I., Rudavin N. 2019 *Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems* Proceedings of 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering pp. 214-219.