PROFESSIONAL PAPER

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

The Model for Assessing the Security Level of Instant Messaging Information Systems

Svyatoslav Sychev, Bauman Moscow State Technical University
Denis Bekasov, Bauman Moscow State Technical University

Address for correspondence: Svyatoslav Sychev, Bauman Moscow State Technical University, Moscow, Russian Federation, e-mail: rk474@yandex.ru

Abstract

The analysis of existing information systems for transmitting multimedia messages is carried out, a generalized conceptual definition for describing the architectures of such systems is proposed. The classification of messaging systems and their architectures is given. The key threats that should be considered when developing messaging systems in various application domains are identified. Based on the analysis of threats, a set of criteria has been determined for assessing the architectures of information systems for transmitting messages. A model which allows to make an assessment of parameters affecting the security of instant messaging information systems based on the characteristics of its elements is proposed.

Keywords

Instant Messaging, Data transmission, Messaging security, Client-server architecture, Peer-to-peer, Simulation modeling, Threat evaluation

1. Introduction

Information systems for transmitting messages have thoroughly entered our everyday lives. We have been using them in various ways since the last century. Nowadays these systems are commonplace. The most widespread kinds are social networks and messengers, and the market for corporate messengers is actively growing. Systems for transmitting messages have found their place in other aspects of our lives such as medicine (Newman & Brownell, 2008), education (Budi, Eileen, Lusiana, & Timothy, 2015) and many others. Of particular note are emergency alert systems as a notification from such a system may be the difference between life and death for some people (Software Engineering Institute, 2013).

Various threats should be considered when developing systems for transmitting messages, for example, the transmission or its contents may be compromised or changed in some way, the messages may be lost or blocked during the transmission, etc. New information security methods and related technologies are constantly being developed and perfected. End-to-end encryption systems, analyzed in (Ermoshina, Musiani, & Halpin, 2016) (Endeley, 2018), have recently become popular. Some other aspects of messenger's security are looked at in (Unger, et al., 2015), (Aziz, Tarapiah, & Atalla, 2018). However, it is impossible to completely eliminate all the threats as they improve alongside security measures.

In general, a focus on a certain number of threats is required when developing systems for transmitting messages. The exact number depends on the task at hand, as does the importance of protecting against each of the threats.

Conducting experiments to detect vulnerabilities using a real system is generally cost- and time-ineffective. It should be noted that such experiments are only possible in the later stages of the development when the cost of a mistake is significantly higher than early on. As such a model which allows determining whether the proposed architecture fits the safety requirements is of particular interest. This article is concerned with the development of such a model.

2. Problem analysis

2.1 Definitions

The concept of a system for transmitting messages is broad and is not limited to messengers or social networks. It can also apply to distributed systems where interaction between modules is done with messages. Consequently, it is proposed to use the following generalized definitions in this article:

- *Node* is an element of the system which receives, processes and sends messages.
- The *data link* is a set of technical tools and transmission medium which allows message transmission between nodes.
- *Message* (package) is a data set transmitted between nodes through data links. It is suggested to abstract from the technicalities of transmissions using particular data links and to view messages as a comprehensive data set. For example, the message should be viewed as a whole and not as a collection of packages during network transmission.

2.2 Classification

Various systems for transmitting messages were analyzed to determine which elements are significant and which basically sets the systems can be grouped into. Such systems can be classified into the following groups in accordance with their application: social networks, general messengers, corporate systems for transmitting messages, specialized systems for transmitting messages and emergency alert systems. According to the systems' structure the following types of architectures can be identified:

- Centralized, or client-server architecture – one or several central high-performance nodes provide basic functionality, the rest of the nodes function as originators or receivers of messages (Schollmeier, 2001). Examples of such architectures are analyzed in (Budi, Eileen, Lusiana, & Timothy, 2015), (Umesh, 2016).
- Based on peer-to-peer networks, where functionality is spread evenly between all the nodes and no client or server machines are defined.

A hybrid approach as described in (Schollmeier, 2001) should also be noted. Such a system uses a peer-to-peer network as a base but needs a central object to provide part of the functionality.

The majority of systems for transmitting messages are centralized, for example, one of the most popular messenger apps WhatsApp. Its architecture is describing in detail in (Umesh, 2016). That said lately even systems with centralized architecture may be comprised of dozens of various nodes based on different servers, which in turn may be located in different data centers. Replication, sharding, and application of micro-service architecture make it impossible to view a server as a single node in a centralized system. As such a model of any system will consist of multiple nodes that exchange messages (important information, service data, control signals).

2.3 Threats

To determine the integral parameters of system elements this article proposes to draw from the following common threats:

- message loss during transmission (network problem, blocking);

- loss of speed during message transmission;
- message transmission discovered;
- message content exposed;
- message content replaced;
- threat of node being accessed or substituted.

In real practice, only threats which are significant to the task at hand are considered. In case of emergency alert systems, for example, the transmission being discovered or even the message contents being exposed is not a primary concern, but message blocking is intolerable.

3. Model

It is proposed to use simulation modelling to evaluate parameters of the system for transmitting messages. Simulation modelling is a method of analysis based on running experiments on the model approximating the system under investigation. Basic principles of simulation modelling are laid out in works (White & Ingalls, 2015). This method of analysis is being commonly used in fields such as data transmission (Bogachev , 2018), logistics (Yassine, Khalid, & Said, 2019) and others.

Many simulation models are built using graphs (Buss, 2001). The architecture of systems for message transmission is similar to a graph which is an added benefit to using such a model. Services, servers and client programs take the form of nodes, and data links take the form of edges. Based on the architectures distinguishing characteristics discussed above and threats to a system for transmitting messages it is proposed to simulate the system as:

- a set of nodes;
- a set of links between the nodes;
- multiple message types.

Sets of nodes and links depend on the systems' architecture. Separate servers, agents of the peer-to-peer system, client apps and services (in case of micro-service architecture) can serve as nodes. The following defining node characteristics are proposed:

- message processing time;
- accepted message type;
- generated message type;
- rules for generating and/or transforming messages;
- probability of message loss;
- probability of error;
- probability of message transmission discovery;
- probability of message contents exposure;
- probability of message contents replacement;
- probability of node malfunction.

A node may serve as a generator (a rule is required by which messages are generated), a transmitter (the node processes messages, spending an amount of time on it, and there are risks associated with messages being lost or compromised, type of message may be changed), and a receiver. Nodes relate to data links which transmit messages. Moreover, each node can transmit a message through one or several data links depending on the systems' architecture. As is the case with nodes, messages are susceptible to threats during transmission. The following data link characteristics, describing common threats, are proposed:

- Message transmission time;
- Error probability;
- Message loss probability;
- Message replacement probability;
- Probability of message transmission discovery;
- Probability of message contents exposure;
- Probability of message contents replacement;

- Probability of data link malfunction.

Message types are added for a more thorough simulation of system interaction with different kinds of messages (text, image, video) and message encryption (message type changes when encrypting in a node). For each message type its own processing times, probabilities of loss and other characteristics may be assigned. Thus, the system architecture is represented by a graph in which messages of different types are being transmitted from node to node.

One should adjust the list of parameters and choose the level of detail for the system appropriate for the given task before applying the proposed model. For example, in case of large system services on a single server may be viewed as a single node. In the case of a system using a relatively small (1-3) number of machines, each service should be viewed as a separate node.

4. Practical application

In this section examples, demonstrating how the proposed model may be used for evaluating various systems' characteristics, are provided.

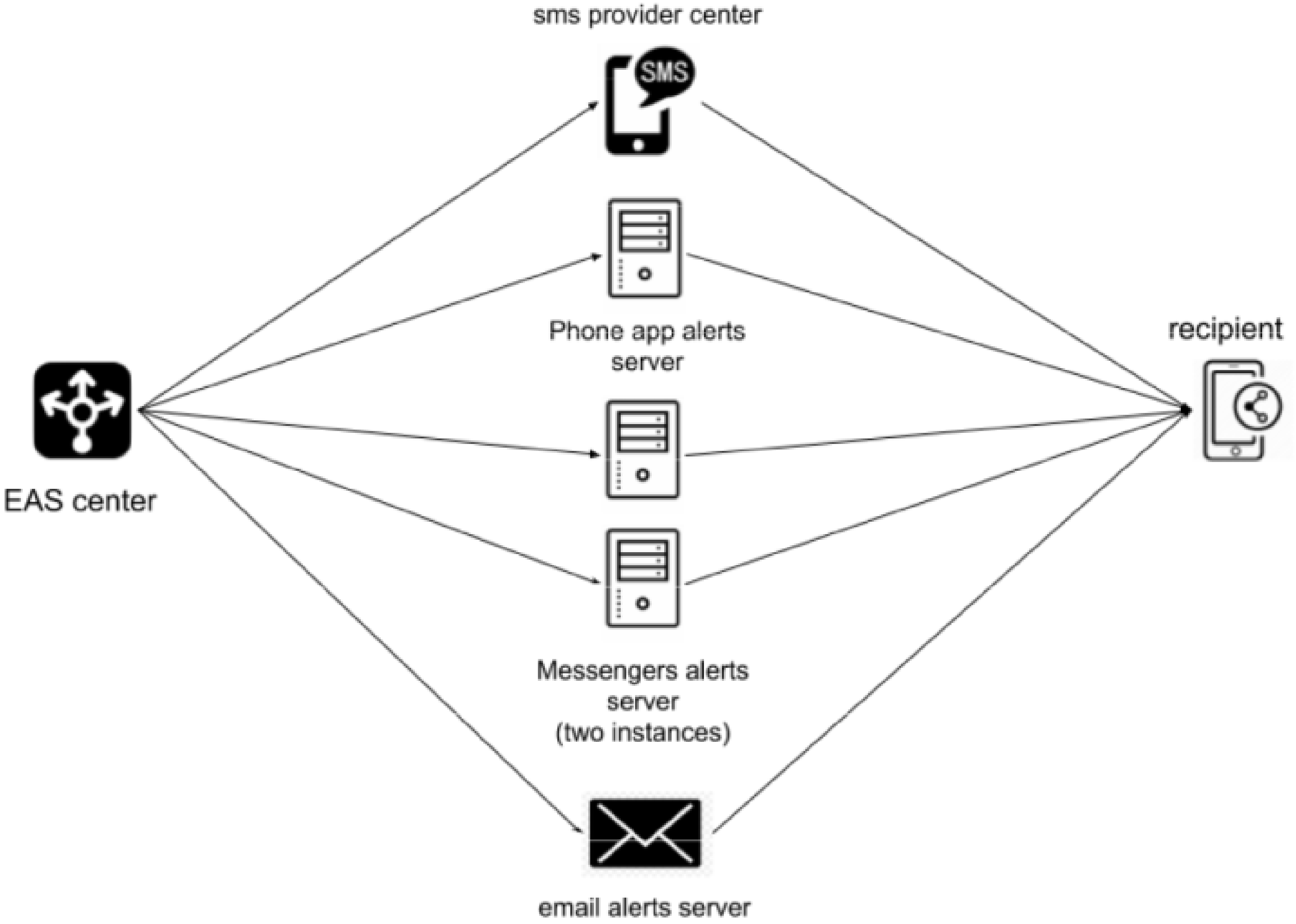

Figure 1. Example of emergency alert system architecture

Figure 1 provides an example of an emergency alert system (EAS) architecture. Emergency alerts are transmitted from EAS center to receivers through SMS, special phone apps, email and various messengers. Separate services/servers are allocated for each of those systems. The most important characteristics when evaluating an

EAS are message transmission speed and probability of message delivery in case of emergency (the probability of node or data ling malfunction is high).

Figure 2 provides an example of a model for such EAS architecture. Nodes of a single type are highlighted with the same color. Probability of message loss, probability of node malfunction, message processing time and other characteristics should be defined for each of the nodes. Similar characteristics should be defined for data links as well.

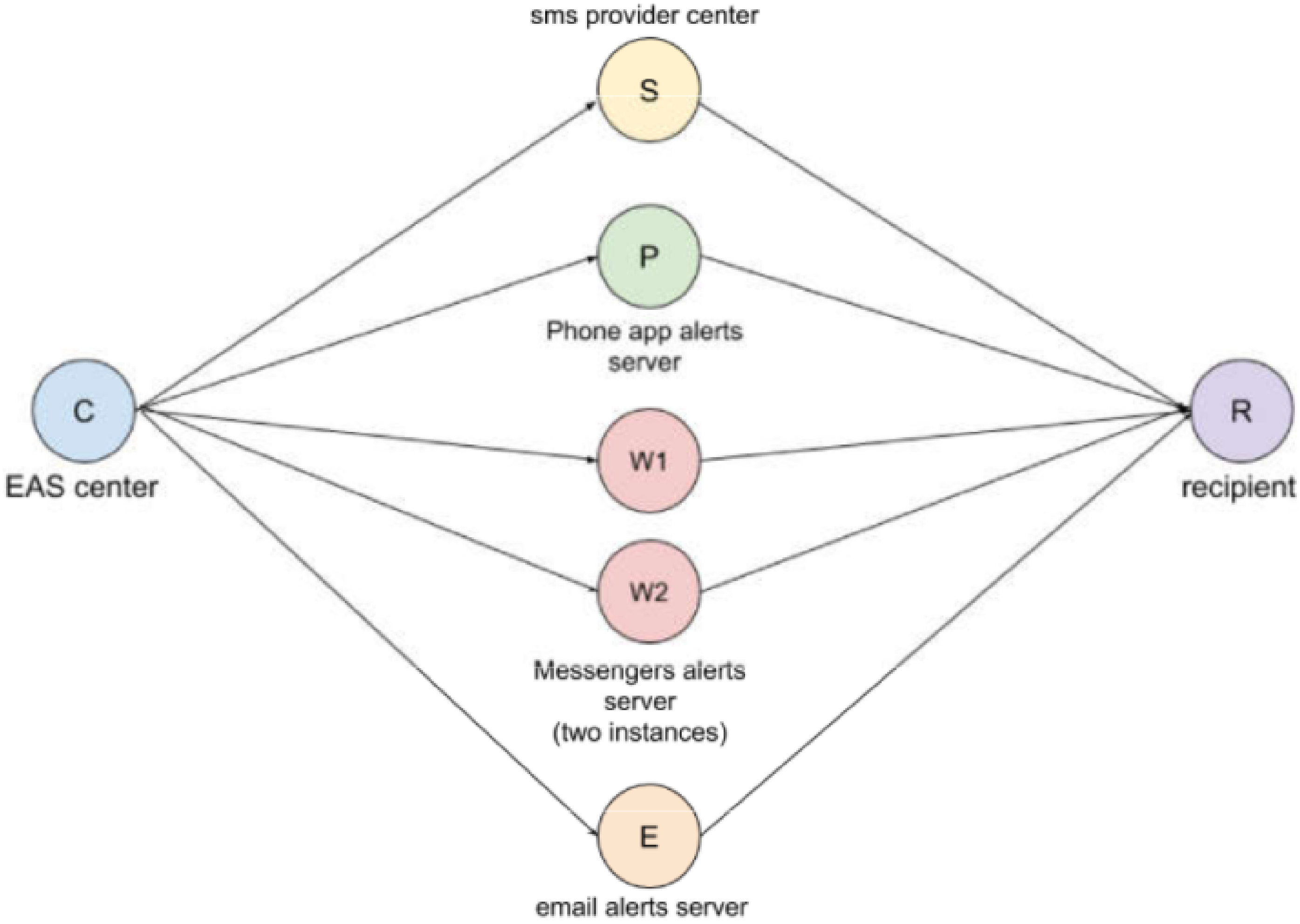

Figure 2. Example of model for system architecture

Based on the proposed model and using the parameters described above, the following characteristics may be discovered:

- Probability of information reaching the receiver (the number of received messages divided by the number of messages sent).
- Maximum information delivery time (without accounting for the complete loss of information).
- Average information delivery time.
- Other statistics data concerning the delivery time needed for system effectiveness evaluation.

An example of the architecture of an abstract region distributed security messaging system is presented in figure 3. Departmental communication systems, government and privately owned military establishments, transnational companies may have such structures.

The example system operates in two regions, between which the data can only be transmitted through regional hubs. Regions are divided into zones. Each of the zones either has its own center to which stationary equipment is connected or local hubs which service even smaller zones or portable equipment. The message routes from sender to possible recipients are portrayed with arrows. It is expected that many recipients may be connected to the hubs.

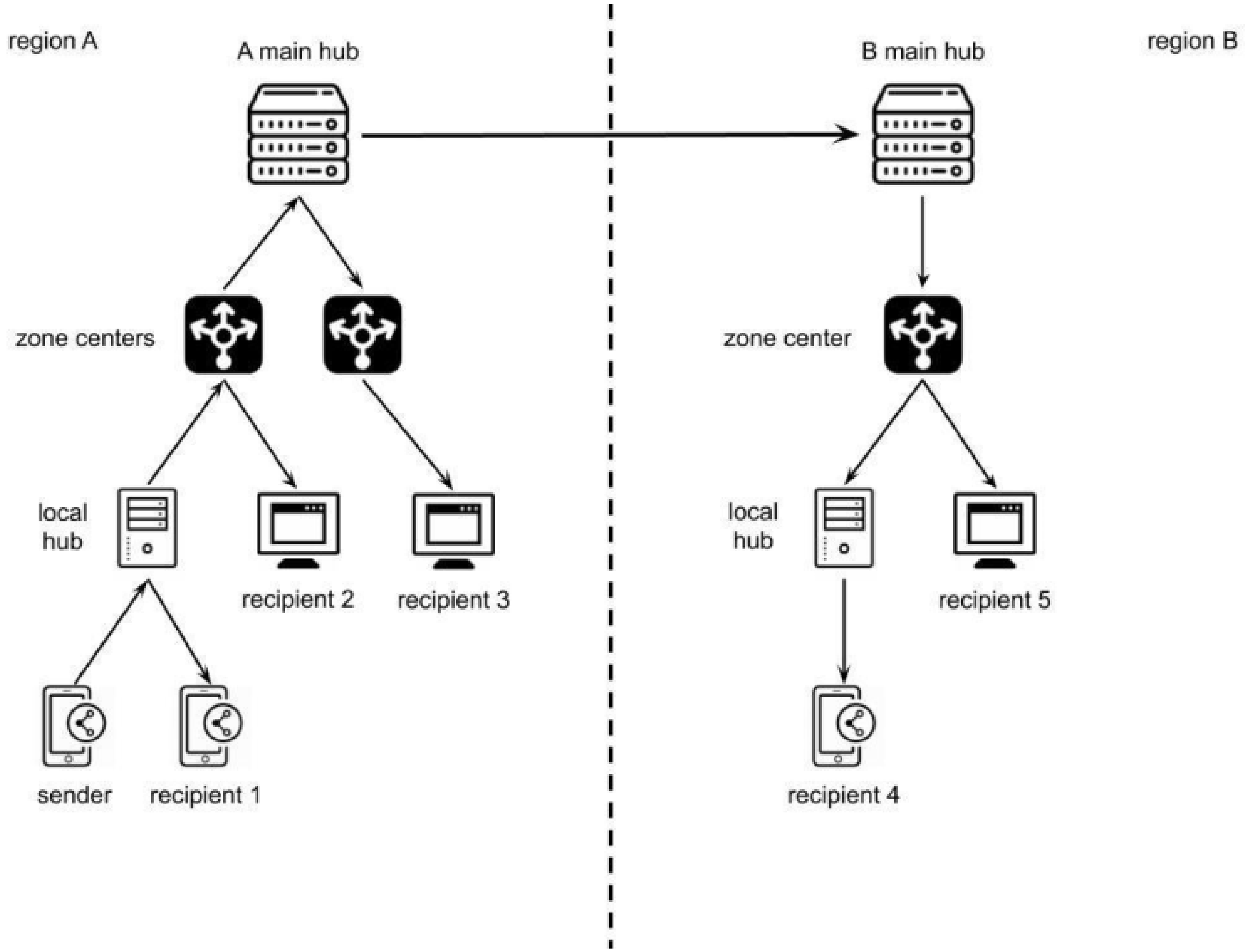

Figure 3. Example of system for message transmission architecture

In such a system with multiple data links and nodes, the problem of security is of utmost importance, especially if the information transmitted is confidential. Time and other parameters discussed earlier are also essential. Evaluation of these parameters is possible with the help of the model presented in figure 4. Modelling can also help determine potential weak points in a timely manner.

This paper is not concerned with methods for determining the characteristics of nodes and data links. This method is a subject for a separate enquiry.

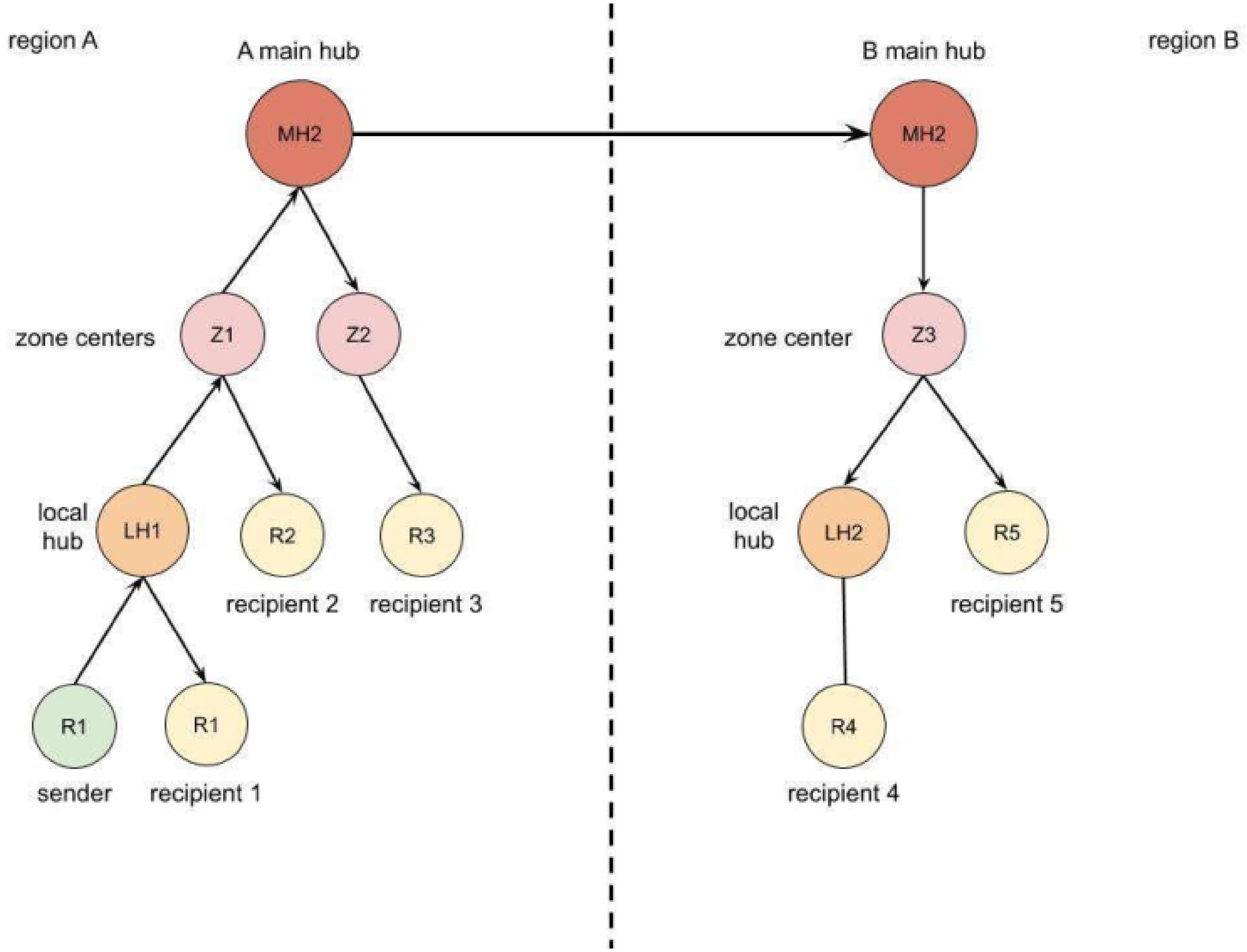

Figure 4. Example of system architecture model

5. Conclusion

After an analysis of threats and characteristics of a system for message transmission architecture, a model was proposed. The proposed model allows for evaluation of the parameters of the system based on the characteristics of its elements. Several model parameters were pointed out. These parameters describe the system's level of vulnerability to the presented threats. The model may be used in different fields of application. Various levels of threat detail and sets of parameters may be chosen depending on the task. The model allows to leave out low-priority parameters and keep only the ones integral to the current task.

The proposed model may be used for:

- analysis of various parameters of the real system in order to detect weak points;
- analysis of the suggested system architecture in the design stage in order to avoid mistakes and ineffective solutions;
- analysis of the modified architecture during revisions and additions of new functions to the system in order to prevent degradation of the system's key par

Usage of the proposed model requires some expenses, mostly to determine node and data link parameters, however, the cost of architectural mistake will be tens or hundreds of times bigger than these expenses.

References

Aziz, K., Tarapiah, S., & Atalla, S. (2018). SIMSSP: Secure Instant Messaging System for Smart Phones. *Lecture Notes in Networks and Systems.*, 647-657.

Bogachev , D. (2018). Simulation model of the information exchange environment, including a mathematical model for reservation of resources of a packet data network with multiple access. *The Eurasian Scientific Journal*.

Budi, Y., Eileen, H., Lusiana, D., & Timothy, A. (2015). Architecture and Implementation of Instant Messaging in Educational Institution. *Procedia Computer Science*, 5-13.

Buss, A. (2001). Basic Event Graph Modeling. *Simulation News Europe, Technical Notes*.

Endeley, R. (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*, 95-99.

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-End Encrypted Messaging Protocols: An Overview. *Third International Conference, INSCI 2016 - Internet Science*, (pp. 244-254). Florence.

Newman, A., & Brownell, J. (2008). *Applying communication technology: Introducing email and instant messaging in the hospitality curriculum.* Retrieved from Cornell University School of Hotel Administration site: htp://scholarship.sha.cornell.edu/articles/1040

Schollmeier, R. (2001). A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. *Proceedings First International Conference onPeer-to-Peer Computing*, 101-102.

Software Engineering Institute. (2013, September). Best Practices in Wireless Emergency. USA.

Umesh, G. (2016). An overview on the architecture of What`s app. *IJCSET.*

Unger, N., Dechand, S., Bonneau, J., Fahi, S., Perl, H., Golberg, I., & Smith, M. (2015). SoK: Secure Messaging. *in Proc. IEEE Symp. Secur. Privacy*, 232–249.

White, K. P., & Ingalls, R. G. (2015). Introduction to Simulation. *Proceedings of the 2015Winter Simulation Conference*, (pp. 1741-1755). Huntington Beach California.

Yang, B., & Garcia-molina, H. (2001). Comparing Hybrid Peer-to-Peer Systems. *Proceedings of the 27th International Conference on Very Large Data Bases* (pp. 561-570). San Francisco: Morgan Kaufmann Publishers Inc.

Yassine, A., Khalid, B., & Said, E. (2019). Supply Chain Modeling and Simulation using SIMAN ARENA a Case Study. *International Journal of Advanced Computer Science and Applications Vol. 10 No. 3*.