BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2020 • Vol. **72**, pp. 41-55
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.72.20.05

State-of-the Art and Trends in Network Security Control

Rosa Fatkieva[1], Elena Evnevich[2], Radoslav Yoshinov[3]

[1,2]Saint Petersburg Institute of Informatics and Automation, St. Petersburg, Russian Federation
[3]Bulgarian Academy of Sciences, Sofia, Bulgaria
Emails: rikki2@yandex.ru, eva@iias.spb.su, yoshinov@cc.bas.bg

Abstract: Network security assurance for data transfer and processing plays significant role in the domain of information security. Presented review deals with current research situation, makes analysis and classification of publications on the topic with regards to scientific, temporal, geographic, etc. aspects in order to determine promising development trends. Publication base Scopus serves as a source for sampling. Analysis and sampling was implemented both in the manual mode and by means of special software for automated search by keywords. Sample could be considered as a representative one: about 2000 publications from more than 1000 sources. Network security research statistical characteristic obtained as a result of analysis were visualized in a graphic form by diagrams of different types. Statistics were represented according to different criteria: problem statement, application domain, publication activity in different continents, countries, attribution to authors, research and industrial organizations, publisher houses, citation index, temporal research activities distribution in the period of 2015-2020 years, etc. Analysis resulted in formation of most relevant set of works, on the basis of which classifications of promising research directions and network security assurance methods were developed.

Keywords: automated keyword search, classification criteria, network security, publication activity, sampling, statistic diagrams.

1. Introduction.

Numerous organizations, scientists and developers around the world make their contribution to the development of network security methods. These activities are to a great extent accounted for growing number, power and territory distribution of

network attacks as well as for automated scenarios of attacks capable of reconfiguration when being unsuccessful.

Under those conditions main development trends and directions are formed for the systems of network security control including monitoring components, methods and models of software-defined and self-organizing networks. Systems of network security control are wide spread in many applied domains thus leading to a need of development and introduction of modeling and methodic apparatus of network security control depending on the specifics of application domain and on control level: on the level of physical components it consists in measuring and monitoring of ultimate equipment; on the level of cyber-physical systems and information computing systems – in development of a complex of operational control models; on the level of intelligent control means – in development of complex of models for strategic network security control. Economic, technological, physical and other limitations as well as problems of interaction maintenance for different information computing systems also make contribution to the problem in the situation of data amount growth and difficulties of data storage, recovery and repeated use. Developers of infrastructures for system interaction using data transfer technologies demonstrate increasing interest in Service–Oriented Architectures (SOA) and in protection of network perimeter under joint use. A tendency appears to wider use of Internet of Things enabling control with wireless data transfer. Introduction of 5G networks is associated with new risks connected with higher virtualization, complications of administration tasks, exploitation of well-known Internet protocols vulnerabilities.

All the above said results in the application of different sets of quality indices for assessment of functioning of network security control in the integrated solutions in the frames of united information space, also depending on the goals and optimization models being used. Therefore a huge amount of conceptions, models and methods of network security control are brought to life in the scientific community.

2. Background: research domain, areas and directions. Materials and methods

Search for publication activities on the topic in the Scopus base was carried out in the manual mode and was supplemented by analysis of representative publications sampling by means of VOSviewer software according to 13604 keywords (Fig. 1).

1999 publications from 1040 sources covering the period of years 20152020 were analysed. Analysed documents were subdivided in types as follows: scientific papers – 666, articles in press – 11, books – 4, book chapters – 65, conference papers – 975, conference reviews – 249, editorial documents – 1, letters – 2, reviews – 26. Analysis has demonstrated that network security was the central theme (798 occurrences). Associative search was implemented by narrowing the subject domain and by carrying out refined search.

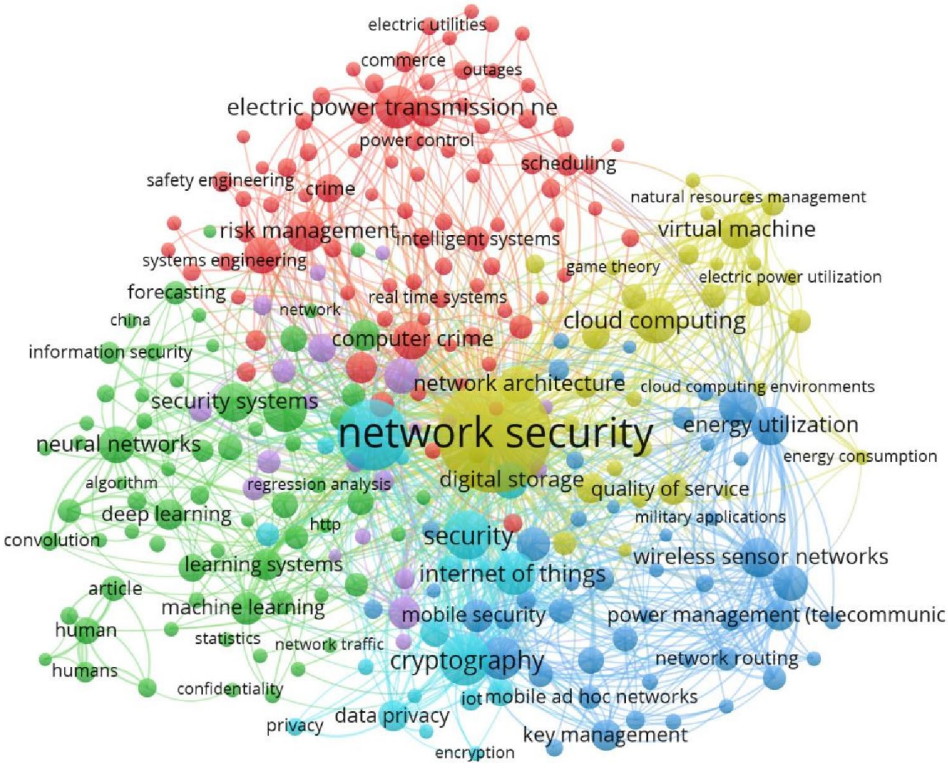

Fig. 1. Main research areas of network security according to Scopus base and sampling by VOSviewer software

Relevant research results were ranged by decrease of occurrence number and as a result several areas (research directions) of network security were outlined. They are as follows:

Information management (number of occurrences – 297 publications) – refers to the organization activities cycle: obtaining information from one or more sources, its storage and distribution by request, and its ultimate storage in the archives or its deleting. Publications devoted to information management could be subdivided into the following sections:

- formation of technological environment of information system;
- information system development and maintenance;
- planning in the information system environment;
- formation of organization structure in informatization domain;
- information systems exploitation;
- formation of innovation policies and implementation of innovation programs;
- personnel management in informatization sphere;
- investment management in informatization sphere;

- formation and complex protection assurance of information resources;
- information flows control.

Security (number of occurrences – 142 publications) – reveals the following network security associations with some security technologies and tools that are relevant to network security control:

- cryptography (165 publications) – represented by information security and users authentication;
- cloud computing (128 publications);
- data security (119 publications) – the area is also closely related to risk management, neural networks, cryptography, Internet of Things, wireless sensor networks;
- Authentication (113 publications) – authentication, access users control;
- Internet of things (113 publications);
- Wireless sensor networks (98 publications);
- Computer crime (89 publications) – crime statistics helps to determine the field of protection and the threats to counteract to;
- Key management (60 publications) – includes asymmetric cryptography;
- Data privacy (60 publications) – information confidentiality.

Publication analysis showed that some of works include both theoretical foundations and practical applications which can be used to ensure security control of a specific network topology. A number of works confirm that network security control depends on network configuration and specification (IoT, wireless sensor networks). Some of publications cover general concepts of network security – information privacy, data security, computer crimes. Other ones are aimed at development of specific tools and methods for network security systems and for the data being transmitted through – cryptography, authentication, key management, cloud computing.

Risk Management (number of occurrences – 97 publications) has the purpose of risk management, minimization of losses in the case of security threats implementation. Publications describe the process of making and implementing control decisions aimed at reducing the probability of information security violations and at minimizing possible damage.

Neural Networks (number of occurrences – 82 publications). Publications describe the use of neural networks as a method of data mining including attribute extraction in attribute-based access control to unstructured text resources and event prediction.

Virtual Machines (number of occurrences – 80 publications) – area covers the network security of virtual machines as part of the network infrastructure including their configuration.

3. Main areas of publication activities and analysis of relevant works

Some research works were grouped according to a certain criterion: by identity of method used (but different implementation or application area), by scope of application (for example 5G networks or wireless sensor networks, etc.), by technology used.

A group of publications is devoted to application of block chain technology to security enhancement. Works [1], [2], [7], [11], [22], [25], [32] describe block chain in creation of secure IoT infrastructure (IoT) and include the following methods:

Method of building distributed cloud architecture using Software-Defined Networks (SDN) [1] addresses the security, scalability, performance and fault tolerance of IoT network. In comparison with the existing models proposed architecture has enhanced performance due to reducing latency and response time, increasing throughput and being able to detect real-time attacks in IoT network.

Method of building Block-VN architecture for transport network (VN) [2]: the proposed distributed transport management system is considered to be applicable to data security and confidentiality issues in transport networks.

More methods of implementation of block chain model in the IoT network: [7] considers application of block chain technology to IoT network in the sphere of medical services in order to ensure security of data and transactions based on extended cryptographic primitives; in [22] – block chain is used in IoT as a system of decentralization to avoid a single point of failure (when authentication of all devices passes through one server).

Method of authentication by electronic signature based on elliptic curves in IoT networks [11] for secure access control to devices.

Method of decentralized access control in IoT networks: the study [25] proposes a BlendCAC method taking into account specific features of the IoT network under protection (need for scaling and decentralization, resource limitations) thus addressing key security challenges of IoT device resources and information.

Method of boundary computing [32] for secure control of IoT devices within a smart home using a distributed block chain-Tor transaction to ensure data confidentiality, generation, storage and shared use.

Besides, block chain technology can be used in intrusion detection methods as described in [4], and in the DDoS-attacks joint mitigation methods [17], which allows using resources of several domains to prevent DDoS-attacks by means of information exchange about attacks in software-defined Networks.

The following methods described in the studies [19], [20], [21], [30] can be distinguished in the context of software-defined networks (in addition to the DDoSattacks joint mitigation method):

Method of measuring network status [19] and real-time monitoring [21] that approaches to security issues in software-defined networks by determining its behavior in order to facilitate control, anomalies detection and troubleshooting.

Method of new-flow attack tracking [20] by reusing asynchronous messages in the control channel and by monitoring the rate of arrival of flow entries. Dynamic access control method use the information obtained to intercept attack flows on the access switch.

Method of anomalies detection and DoS/DDoS-attacs identification named HWDS (Holt-Winters for Digital Signature) combined with the autonomous model of game theory decision-making. Taking into accountcollected data and data obtained by imitation of attacks the method makes possible to mitigate the consequences and to protect software-defined networks from "denial of service" attacks.

Group of works aimed at ensuring security in mobile 5G networks was also identified. Studies [6] and [8] consider the method of joint suppression using artificial noise to ensure safe communication in NOMA CR (non-orthogonal multiple access and cognitive radio) and the method of identification and authentication control taking into account the requirements and specifics of 5G networks.

Methods of network security control in wireless sensor networks (WSN) are discussed in publications [3], [16], [28].

Research [3] provides a simplified three-factor key authentication and negotiation protocol based on Rabin's cryptosystem to protect sensors from Internet attacks.

Paper [16] considers the issue of secure routing in wireless sensor networks to avoid data loss and proposes a trust protocol (TDP). Routing in this protocol is performed in four stages: topology management using k-mean algorithm, communication quality assessment, profiling (tagging of nodes), selection of the most secure path for routing based on labels set in the previous stage.

The publication [28] discusses the protection of wireless sensor networks against denial of service attacks to ensure resource availability in different ways: deployment of the protection system on nodes, construction of a secure network structure, detection of anomalies.

The following group of methods can be described as methods of establishing and managing trust: for special transport networks (VANET) based on fuzzy logic [10], based on block chain technology [13]; for wireless sensor networks [36]; for IoT networks [23], [34], including intrusion detection via traffic sampling [26].

The following publications consider authentication by establishing trust to ensure the integrity, confidentiality and reliability of applications in the transport network [10], [13]; introducing secure trust-based IoT architectures using the name resolution service [23]; intrusion detection systems for protection from attacks by trust control between traffic-sampled Bayesian devices [26]; secure routing in the

wireless sensor networks with a trust mechanism that allows to exclude/include nodes in the routing operation depending on the estimated trust value [36]. Work [5] provides an overview of machine learning methods including issues of network exploitation and control for specific network areas and technologies, among them: traffic forecasting, routing, congestion management, resources, failures, quality of service (QoS), security, statistics and quality assessment.

Paper [9] discusses the Distributed Reputation Management (DREAMS) method for a transport network where network servers are used to perform local vehicle reputation management tasks. This method detects "misbehavior" and recognizes the vehicle where it was detected.

Migration method in Network Function Virtualization (NFV) architecture [12]: NFV is a network architecture that implements network functions in software running on a set of shared servers. The purpose of the network migration method is to optimize energy consumption depending on the intensity of requests.

Publication [14] discusses the problem of security violation in networks through the application of social engineering methods. The main way to counteract the violations is training of personnel (including those responsible for critical infrastructure facilities); the authors present a security training system that can be used to counter social engineering threats (phishing, pretexting, etc.).

Paper [15] focuses on cloud computing. Cloud networks are vulnerable to various network attacks and lack data privacy. To solve security problems there is a need of mechanisms of identity and access control, authentication. The paper suggests some methods for solving these problems and provides a comparative analysis of them.

The study [24] examines and compares queue management methods such as Drop-Tail, Random Early Detection (RED), and Random Exponential Marking (REM) which are used to protect ad hoc networks from DDoS-attacks.

Network data collection methods for real-time monitoring are used to protect networks from attacks and intrusions and to control traffic. A comparative analysis of existing data collection methods was carried out in [31].

The study [35] provides an overview of key management methods in SCADA networks (Supervisory Control and Data Acquisition) that play an important role in critical infrastructures. In order to ensure security in these networks, key management schemes have been developed and their comparative analysis is carried out.

In addition to the above mentioned methods aimed at network security control in IoT some works could be also referred to this group [18], [27], [29], [33], [37]. These studies consider networking technologies, relationships between network protocols and IoT applications [33]; review the security problems of Smart Cities information due to the broad communications network [29]; present method of traffic redirection to ensure confidentiality in IoT network [27], method of transfer control based on protocol PVPIPv6 with secure routing [18] for Smart

Homes and method of secure response to requests aimed at protection against collusion attacks [37].

Papers [38-42] explore 5G networks issues including that of the use of battery-free wireless sensors for cyber-physical systems of state monitoring. Through the wireless power transfer interface the functionality (on/off) of the sensitive node, its measurements and communication periods can be monitored.

Analysis of a representative sample of studies allows to form classification of research directions in the field of network security (Fig. 2) (numbers in square brackets make reference to the source in which this segment is considered), and classification of methods of network security Fig. 3).

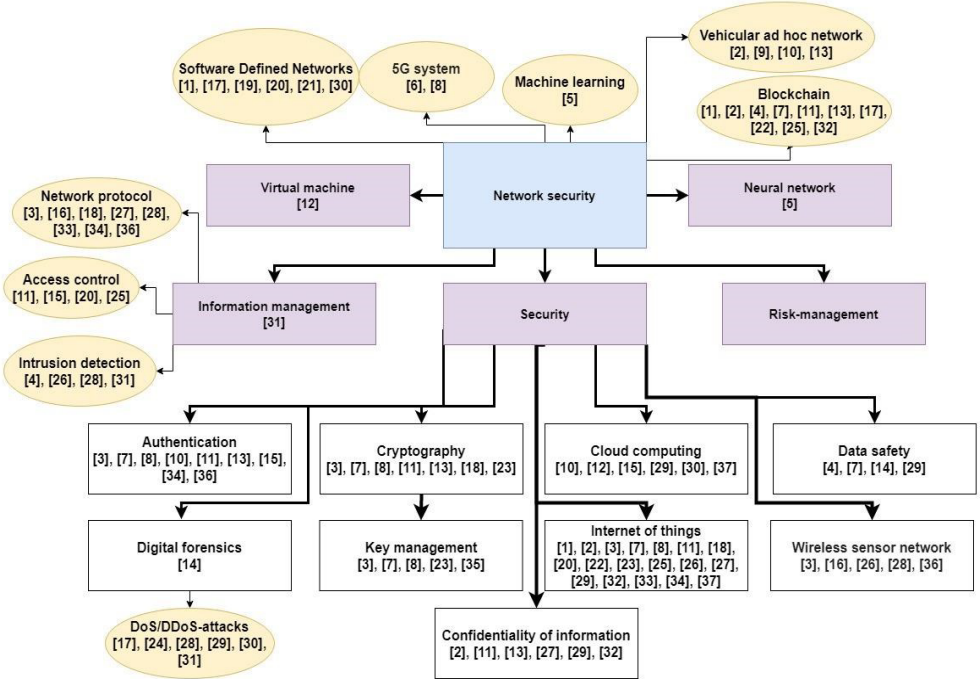

Fig. 2. Classification of research directions in the domain of network security

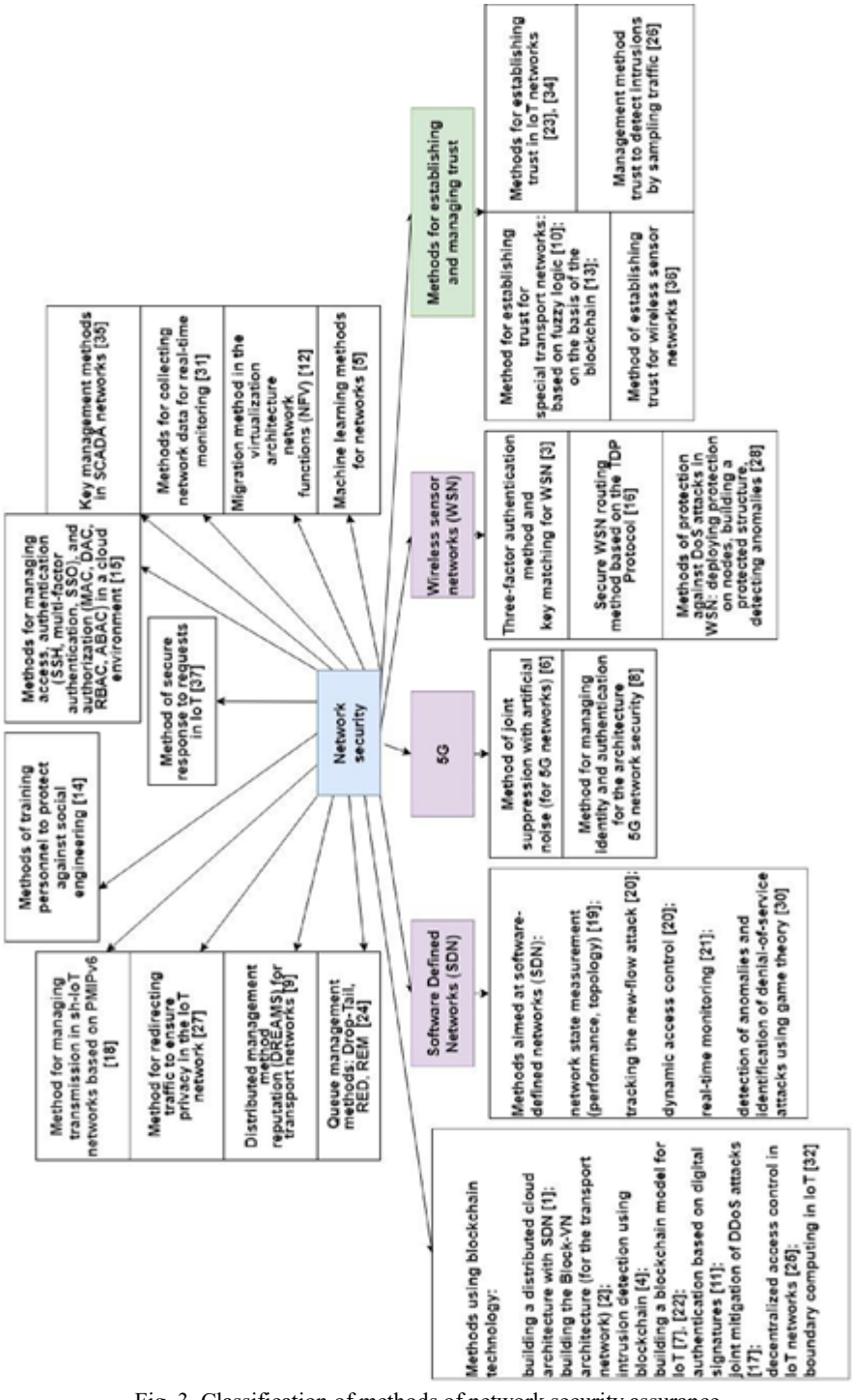

Fig. 3. Classification of methods of network security assurance

4. Research perspective

Presented in the previous section classifications of directions and methods of network security control reveals research trends and also provides distribution of the ownership of research. Growth of number of publications on the topic “Control of network security” is about 4.9 times since 2015 in total and makes possible to trace changes in the publications activities by countries and continents. Statistics presented (Fig. 4) demonstrate that China has taken the lead in network security control research and publications. It is followed by the United States, India, the United Kingdom, South Korea, Canada, and Russia.

Fig. 4. Publication activities: a) on the continents and b) in the countries

As regards publication types (fig. 5) conference documents prevails: 54.3%, followed by papers: 38.6% and book chapters: 2.4%.

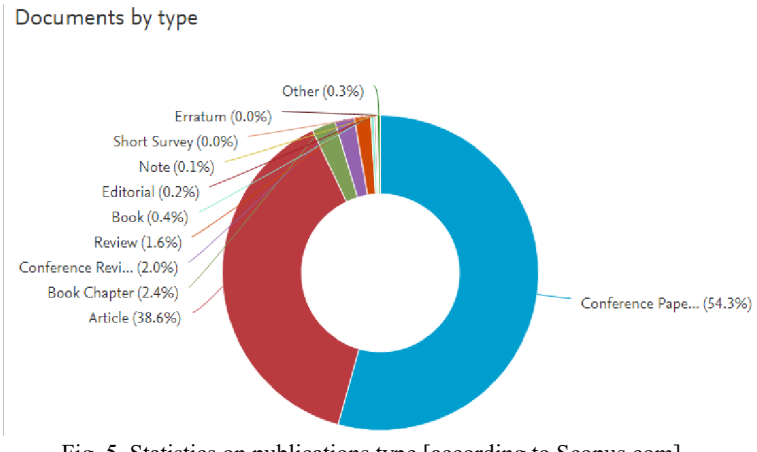

Fig. 5. Statistics on publications type [according to Scopus.com]

The peak of publication activities has taken place in 2019. In April 2020 the leader in publications number was the journal "Advances in Intelligent Systems and Computing". The top ten organizations by number of publications (according to Scopus.com) also include universities and academies of China, institutes of India and a university located in Saudi Arabia.

The analysis showed that both inductive and deductive approaches to multilevel control of network security are being developed. Methods and technologies of multilevel neural network modeling of observed changes in computer network structures and processes are being developed. There is a tendency to interdisciplinary approaches application with the introduction of elements of mathematical and biological structures. Methods of self-organization of network structures are formed using software-defined distributed network structures with prescribed level of trust. In order to find suitable self-protection options it is necessary to develop new methods of multilevel automated synthesis of structurally complex elements of distributed heterogeneous networks. The use of heterogeneous distributed networks and the need for distributed information processing puts forward new challenges in such areas of network data transfer as control of power transmission through wireless and sensor networks, formation of dynamic network infrastructure, self-healing systems. Characteristics of "established" and promising directions is presented in Table 1.

Table 1. Promising research directions on network security

Direction	Relevant topics	Promising directions
Sensor nodes	Mobile telecommunication systems, Internet of Things, Routing protocols	Data structures in sensor networks, « Bloom filters, Network dynamic infrastructure, etc..
Authentication	Internet of things, Authentication protocols, Public key cryptography	Dynamic authentication in mobile networks, Wireless body area network (WBAN), Mobile network computational efficiency, etc.
Network layers	Physical security layer, Intelligent systems, Bandwidth	Computational complexity, Simultaneous Wireless Information and Power Transfer (SWIPT), Energy harvesting and Energy transfer
Network security control	Network protocols, Internet of Things, Energy efficiency, Energy Consumption	Wireless mesh networks, Environmental conditions, Multilevel automated synthesis, Predictive modelling, Self-healing systems
Wireless sensor networks	Wireless sensor networks	Wireless sensor networks interoperability, Middleware, Key agreement protocol
Cryptography	Security, Wireless networks, Mobile security	Queueing networks, Cryptographic primitives, Public key infrastructure for IoT, Trust networks, Distributed perimeter protection
Wireless telecommunication systems	Wireless communications	Open systems, Handover authentication, Network coding
Heterogeneous networks	HTTP	3GPP

Analysis of promising directions of network security automated control showed that the development is complicated by very large numbers of heterogeneous devices and real processes in the networks and their corresponding characteristics. Computational complexity of solving such problems is in direct proportion to the square of the number of devices and conditions to be analyzed. When the number of such conditions is measured in thousands then creation of practical models in a reasonable time by means of existing methods becomes problematic. Overcoming the problem requires development of optimization methods taking into account the variety of the pursued purposes of control of network security, protection and recovery. There is a need for appropriate methods and technologies of real-time automated synthesis of models of computer networks as self-healing cyber security objects with prescribed specific features. One of the promising approaches to the development of synthesis theory and technologies consists in multilevel automated synthesis of reconfigured network security models. Development of methods and technologies of multilevel automatic synthesis of network security models would enable both taking into account the changes in network functioning laws and ensuring flexibility and reduced complexity of problems of networks behaviour prediction as well as providing more information and time for development and implementation of expedient measures of network security control.

5. Conclusion

Analysis of publications on network security control confirms urgency and relevance of the scientific direction. Significant activities is focused on development of methods of network security control by means of block chain architecture, games theory with respect to both tasks of network security control and those of intruder models creation. Application domain of methods of distributed reputation control based on IoT and wireless sensor networks is permanently enlarging. Application space of machine learning methods intended for intrusion detection by network traffic analysis is being formed. Strengthening trends are observed in the area of intruder dynamic profile creation by methods of social engineering. Separate direction of research is formed in the area of digital forensics making possible detection of attacks traces in the network traffic. Development trends analysis enables to form the insight of perspectives in network security domain, in particular, in promising dynamic methods strategy in network security control permitting security control automation. Solution of the above class of tasks in the future would enable to move on to automated synthesis of computer networks in the form of self-healing cyber secure objects. Further development of this direction would form the methods of real-time building/rebuilding of multilevel computer networks models being adequate to current situation and taking into account all the methods and research directions presented earlier. In this case

general problem of synthesis is decomposed into the set of individual tasks each of them having relatively low complexity level and its own application domain.

Acknowledgment

This work is supported by National Science Program “Information and Communication technologies for unified Digital Market in Science, Education and Security”.

References

1. Sharma, P.K., Chen, M.-Y., Park, J.H.: A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE, art. no 8053750, 115-124 (2018).
2. Sharma, P.K., Moon, S.Y., Park, J.H.: Block-VN: A distributed blockchain based vehicular network architecture in smart city. Journal of Information Processing Systems 13(1), 184-195 (2017).
3. Jiang, Q., Zeadally, S., Ma, J., He, D.: Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE, art. no 7870585, 3376-3392 (2017).
4. Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y., Han, J. When intrusion detection meets blockchain technology: A review. IEEE, art. no 10179-10188 (2018).
5. Boutaba, R., Salahuddin, M.A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., Caicedo, O.M.: A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. Journal of Internet Services and Applications 9(1), art. no 16 (2018).
6. Zhou, F., Chu, Z., Sun, H., Hu, R.Q., Hanzo, L.: Artificial noise aided secure cognitive beamforming for Cooperative MISO-NOMA using SWIPT. IEEE Journal on Selected Areas in Communications 36(4), 918-931 (2018).
7. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors (Switzerland) 19(2), art. 326 (2019).
8. Fang, D., Qian, Y., Hu, R.Q.: Security for 5G mobile wireless networks. IEEE Access, 6, 4850-4874 (2017).
9. Huang, X., Yu, R., Kang, J., Zhang, Y.: Distributed reputation management for secure and efficient vehicular edge computing and networks. IEEE, art. no 8094861, 25408-25420 (2017).
10. Soleymani, S.A., Abdullah, A.H., Zareei, M., Anisi, M.H., Vargas-Rosales, C., Khurram Khan, M., Goudarzi, S.: A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE, art. no7995031, 15619-15629 (2017).
11. Cha, S.-C., Chen, J.-F., Su, C., Yeh, K.-H.: A blockchain connected gateway for BLEBased devices in the internet of things. IEEE, art. no 24639-24649 (2018).
12. Eramo, V., Ammar, M., Lavacca, F.G.: Migration energy aware reconfigurations of virtual network function instances in NFV architectures. IEEE, art. no 4927-4938 (2017).
13. Lu, Z., Liu, W., Wang, Q., Qu, G., Liu, Z. A privacy-preserving trust model based on blockchain for VANETs. IEEE, art. no 8428638, 45655-45664 (2018).

14. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., Baker, T.: Security threats to critical infrastructure: the human factor. Journal of Supercomputing 74(10), 4986-5002 (2018).
15. Indu, I., Anand, P.M.R., Bhaskar, V.: Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal 21(4), 574-588 (2018).
16. Karthick, S. TDP: A novel secure and energy aware routing protocol for wireless sensor networks. International Journal of Intelligent Engineering and Systems 11(2), 76-84 (2018).
17. Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., Stiller, B. A.: Blockchain-based architecture for collaborative DDoS mitigation with smart contracts. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 10356 LNCS, 16-29 (2017).
18. Shin, D., Sharma, V., Kim, J., Kwon, S., You, I.: Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT Networks. IEEE, art. no. 7937789, 11100-11117 (2017).
19. Zhang, H., Cai, Z., Liu, Q., Xiao, Q., Li, Y., Cheang, C.F.: A survey on security-aware measurement in SDN. Security and Communication Networks, art. no. 2459154 (2018).
20. Xu, T., Gao, D., Dong, P., Zhang, H., Foh, C.H., Chao, H.-C.: Defending against NewFlow attack in SDN-based internet of things. IEEE, art. no. 7847329, 3431-3443 (2017).
21. Bakhshi, T.: State of the art and recent research advances in software defined networking, Wireless Communications and Mobile Computing, art. no. 7191647 (2017).
22. Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.B.: Blockchain with internet of things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications 10(6), 40-48 (2018).
23. Liu, X., Zhao, M., Li, S., Zhang, F., Trappe, W.: A security framework for the internet of things in the future internet architecture. Future Internet 9(3), art. no. 27 (2017).
24. Wei, W., Song, H., Wang, H., Fan, X.: Research and simulation of queue management algorithms in ad hoc networks under DDoS attack. IEEE, art. no. 7876739, 27810-27817 (2017).
25. Xu, R., Chen, Y., Blasch, E., Chen, G. BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the IoT. Computerss 7(3), art. no. 39 (2018).
26. Meng, W., Li, W., Su, C., Zhou, J., Lu, R.: Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data. IEEE, art. no 72347243 (2017).
27. Liu, J., Zhang, C., Fang, Y. EPIC: A differential privacy framework to defend smart homes against internet traffic analysis. IEEE Internet of Things Journal, 5(2), 12061217 (2018).
28. Osanaiye, O.A., Alfa, A.S., Hancke, G.P.: Denial of service defence for resource availability in wireless sensor networks. IEEE, art. no 6975-7004 (2018).
29. Aldairi, A., Tawalbeh, L.: Cyber security attacks on smart cities and associated mobile technologies. Procedia Computer Science 109, 1086-1091 (2017).

30. De Assis, M.V.O., Hamamoto, A.H., Abrao, T., Proenca, M.L.: A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. IEEE, art. no. 7923413, 9485-9496 (2017).
31. Zhou, D., Yan, Z., Fu, Y., Yao, Z.: A survey on network data collection. Journal of Network and Computer Applications 116, 9-23 (2018).
32. Rahman, M.A., Hossain, M.S., Loukas, G., Hassanain, E., Rahman, S.S., Alhamid, M.F., Guizani, M.: Blockchain-based mobile edge computing framework for secure therapy applications. IEEE, art. no. 8534320, 72469-72478 (2018).
33. Triantafyllou, A., Sarigiannidis, P., Lagkas, T.D.: Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends Wireless Communications and Mobile Computing. art. no. 5349894 (2018).
34. Ud Din, I., Guizani, M., Kim, B.-S., Hassan, S., Khan, M.K.: Trust management techniques for the internet of things: A survey. IEEE, art. no. 8531615, 29763-29787 (2019).
35. Rezai, A., Keshavarzi, P., Moravej, Z.: Key management issue in SCADA networks: A review. Engineering Science and Technology, an International Journal 20 (1), 354-363 (2017).
36. Ishmanov, F., Bin Zikria, Y.: Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues. Journal of Sensors, art. no. 4724852 (2017).
37. Li, G., Wu, J., Li, J., Guan, Z., Guo, L.: Fog computing-enabled secure demand response for internet of energy against collusion attacks using consensus and ACE. IEEE, 11278-11288 (2018).
38. Perera, Th. D. P., Jayakody, D. N. K.; Sharma, Sh. Kr., Chatzinotas, S.: Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges. IEEE Communications Surveys & Tutorials 1, 264-302 (2018).
39. Rajaram, A., Khan, R., Tharranetharan, S., Jayakody, D.N.K., Dinis, R., Panic, S. Novel SWIPT schemes for 5G wireless networks. Sensors, 19(5), art. no. 1169 (2019).
40. Ali, K., Nguyen, H.X., Vien, Q.-T., Shah, P., Chu, Z.: Disaster management using D2D communication with power transfer and clustering techniques. IEEE, art. no. 14643-14654 (2018).
41. Loubet, G., Takacs, A., Dragomirescu, D.: Implementation of a battery-free wireless sensor for cyber-physical systems dedicated to structural health monitoring applications. IEEE, art. no. 24679-24690 (2019).
42. Jouhari, M., Ibrahimi, K., Tembine, H., Ben-Othman, J.: Underwater wireless sensor networks: A survey on enabling technologies, Localization Protocols, and Internet of Underwater Things. IEEE, 96879-96899 (2019).