Secure Routing in IoT with Evolutionary Algorithm

Alireza Ebrahimi Basabi, Jingsha He, and Seyed Mahmood Hashemi

***Abstract*—The degree of communication security is dependent to the secure routing. Any threat to the assets (hack in generality) decreases the security, so we can say security is the inversion of hack probability. In other words, security is increased with the reduction of hack probability. One major method to decrease the hack probability is finding the appreciate the path that is declared in secure routing. There are multiple effective parameters for secure routing. The aim of this paper is studying types of hacks and then presenting a useful optimization formula that considers all parameters. Multi-objective Imperialist Competitive Algorithm (MOICA) solves the presented model of secure routing.**

***Index Terms*—Communication, secure routing, optimization.**

I. Introduction

Undoubtedly security is an important issue for the communication; so many researches are assigned to the network security field. However, we cannot have a fully secure system, produce a high degree of security is desirable. Nevertheless, existence complexity of the network communication (including many details) in one side; and various network applications been in another side [1], and different types of attacks in other side cause consanguineous failure works [2]. Therefore, there is a need to an approach that combines required elements for the network security in the one structure and without involving to details and without loss of generality.

We can divide information security into two major fields: 1-data security and 2- network security. Data security is based on cryptography theory and researches about confidentiality, integrity, and availability. Network security is based on security protocol, mechanism, and services. There are two types of the network environment: 1- public such as the Internet and 2- enterprise such as electric power dispatching network (SPDnet). Study of attacks allows us to increase security. Although attacks are in the wide range, this paper focuses on structural attacks. Structural attacks mean attacks that use wrong information of the network structure and done bad behavior base on their information. Selective, Sybil, Sinkhole and Wormhole are famous types of these attacks.

The aim of this paper is providing a secure routing approach base on the right information about the network structure. The proposed problem is based upon the dynamic model so it can adapt to the network circumstance easily.

The rest of this paper is organized as follow: Section II is assigned to the Related Works. Section III studies the topology of structural attacks. Section IV describes the proposed approach and also its present its results and finally, Section V is the conclusion.

Manuscript received July 12, 2019; revised November 11, 2019.

The authors are with Beijing University of Technology (BJUT), China (e-mail: touraj_ebr@yahoo.com).

II. Related Work

Although security may be related to the many details [3], [4], considering all of them cause to increasing of the computing volume. Thus, we must consider just the most effective parameters. Previous works on this field, help us to find desirable parameters.

Authors of [5] consider security and time performance and they propose an algorithm, named as Attack Resilient and Retrieval Time trade-off strategy (ARRT), to produce tradeoff between parameters. Time in their algorithm is the variable of reading request. They suggest security as centrality and define it as a number of shortest paths between two selective nodes (server and client).

Laura Dios *et al.* right her paper base on the Markovitz theory with two aspects: risk and return [6]. Return can be considered as access request. She supposes a case that return rate and of assets are uncertain.

Authors of [7] focus on the biometric system that must select parameters to increase the effectiveness of the network. They do this task with an Evolutionary Multi-Objective Algorithm to optimize the threshold to determine the Global error of False Acceptance (GFA) and Global error of False Rejection (GFR). In the system with assets, clients send an access request to the server and then the server may accept or reject their request base on the security of the system. Accept/Reject access request can be the translation of GFA/GFR.

Valentina Viduto *et al.* present an approach base on investment cost and risk of possible degradation of CIA [8]. They define the initial risks as impact transactions on vulnerabilities and then calculate the total risk with the summation of initial risks. Nimmy Cleetus *et al.* study the Information Gain that determines the feature for classification using entropy value [9]. Ram Mohan Chintalapalli *et al.* proposes a combination Lion Algorithm (LA) and Whale Optimization Algorithm (WOA), named as M-LionWhale, to secure routing based on some parameters [10]. Their parameters are trusted degree, link lifetime, energy and mobility. Since they do not use dominance in their approach, they put all objects in one formula with the same weight. Their different objects have different nature and affect secure routing with different weight, so combining all of them in one formula cannot produce proper results.

Razieh Rezaee *et al.* a combination of Abstract Security Model (ASM) and Network Security Model (NSM) in a Unified Modeling Language (UML) based approach [11]. Because their work is based on the static privilege and

doi: 10.18178/jacn.2019.7.2.270

scoring, it can not be adapted on the network with dynamic circumstances in the real world.

Masoud Hayeri Khyavi *et al.* count number of important parameters to create an application with more security.

Zhiyong Lu *et al.* present characters of the network security (such as confidentiality, integrity, and availability) as vectors and then propose a model to evaluate them [12]. They present these characters with Eigenvalues, then the total security of the system is evaluated with the hierarchical system of N hosts.

However, the above hierarchical system can indicate the security of the system, the evaluation of the security needs to score the network security by experts. Authors propose number formulas to scoring the network security, but the proposed formulas have a non-examined coefficient that reduces the efficiency of the proposed formulas.

Haihui Ge *et al.* propose a model to evaluate the network security base on the attack graph [13]. Their model has a risk function with three parameters: 1-asset loss, the 2-threat value of attack and 3- coefficient of attack importance.

Xuanxia Yao *et al.* suppose some parameters for secure routing [14]. The first parameter is energy that they calculate it base on the proposed formula of Long Gan *et al.* [15], so if the node i wants send k bits its required energy is: $E_i(k) = E_{elec}.k + E_{amp}.k.d^2$ where $E_{elec} = 50\ {}^{nj}/_{bit}$, $E_{amp} = 100\ {}^{pj}/_{bit/m2}$ **and d is distance.**

The second parameter is the trust ratio that they calculate it with the division the number of retransmitted packets from node i to node j, on the number of forwarded packets base on the formula of Cheng Weifang *et al.* [16].

The biggest challenge in routing, sending a data packet from source to the final destination in the network is secure, because various forms of threats and attacks cause users will feel insecure to share their private data in the network applications. David Airehrour *et al.* [17] explore different routing protocols and their vulnerabilities. They believe there are two key roles in the network revolution: 1-security and 2-energy consumption. They list 25 vulnerabilities for HP: 1-privacy issue, 2-inadequate authorization/authentication, 3-absence of transport encryption/standard, 4-Web interface vulnerabilities and 5-software/firmware vulnerabilities. The Internet Engineering Task Force (IETF) introduces protocols for routing, but there number of threats to routing protocols. An example of threats of routing is transmitting a large amount of false route information to the node neighbors, to cause an overflow of the routing table. In AODV, which is routing protocol, there is a sequence number to avoid this threat. However their list is useful, none of the protocols can cover different threats. Huanlai Xing *et al.* study routing in the multicast manner [18]. In their paper, data is transmitted in a coding way, so they use the multi-objective evolutionary algorithm to optimize data recombination in the Network Coding based Multicast (NCM).

III. Topology of the Attacks to the Network Structure

These attacks mean routing process is sabotaged with adversary [19]. In other words, when a sender wants to send a data packet to another node, a routing topology procedure decide the proper path in the network base on the information of the network topology, but in the mention attacks routing procedure does not work correctly. The wrong results of executing of the routing procedure is caused by the wrong information of the network topology. The Fig. 1 depicts this problem.

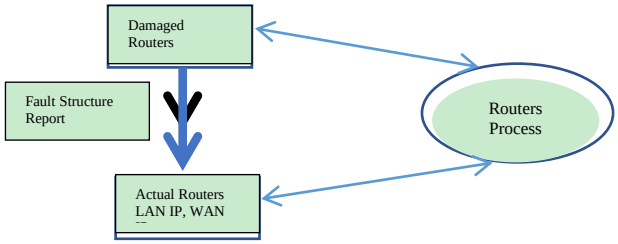

Fig. 1. Topology of the network attacks.

IV. Proposed Model

To prevent the network attacks, there is a need to the correct information about the network structure. In other words, the network application is secure as having as correct structural information. Since the security concepts in the network are independent of each other, we cannot combine all of them in one formula, but the multi-objective optimization model can consider all of them simultaneously. The multi-objective optimization model can produce the required structural information because we assign the important functions for it. To construct the multi-objective model, the important characters of the network are considered. Actually, the backbone of the network has many components, but nodes and links are the most important of them. In addition, links have security characters. Confidentiality, Integrity, and Availability are the most important characters for the links and some values can be considered for them. Thus, the model is the set (V, L). V is set f nodes. L is a set of links. Each link has three values to present Confidentiality, Integrity, and Availability. The routing problem in this model is defined as an optimization problem:

$$Opt.Conf(l1,l2,\dots,ln), Inte(l1,l2,\dots,ln), Avai(l1,l2,\dots,ln) \quad (1)$$

where Conf, Inte, Avai are confidentiality, integrity, and availability of links in the network respectively. In other words, 1 says the routing is a tradeoff between different concepts of security in the network. The other parameters that are studied in the Related Works section, can be covered in the parameters of 1. For example, Avai (availability) includes energy. The major advantage of 1 is considering the parameters independently.

There are many algorithms to solve 1, but Multi-Objective Imperialist Competitive Algorithm (MOICA) is used in this paper.

MOICA is same as other swarm intelligence algorithms initiate with a number of random solutions, which are called Country. According to objective functions, each country has own potential ability. Countries are assigned to Imperialists,

which are the countries with the most ability. The number of imperialist countries is determined with the developer. In the next step, countries change their state (imperialist/colony) or their imperialist country base on their probability value, which is assigned to countries base on their potential ability. In this step, countries are divided with Dominance formula and non-dominated countries are kept in the archive. In the last step, countries try to be simulated as their own imperialist country. The mentioned steps are done until the termination conditions.

V. Experimental Results

Let's there is a network with 20 nodes. Each node has links to other nodes. The problem is finding the proper path to communicate between the first node (named as 'A') and the last node (named as 'Z'). The 1 is used to find the proper path and MOICA is used to solve the 1. Table I, displays the result of the proposed algorithm in 5 different runnings.

TABLE I: Results

	No.of Loops	path	confidentiality	Integrity	Availability
1	20	'A','B','E','Z'	0.986	0.948	0.091
2	15	'A','B','Z'	0.857	0.576	0.384
3	12	'A','D','X','E','Z'	0.348	0.768	0.849
4	30	'A','B','E','G','Z'	0.684	0.542	0.278
5	35	'A','F','R','E','W', 'Z'	0.732	0.675	0.564

Since MOICA has stochastic structure, the final result in any running may be different to others, but we can take a general opinion. The highest number of iteration may cause to produce a better result. The reduction of objective functions has an effect on the final result because the less number of objective functions decrease the probability of non-dominance. We examine MOICA with 20 random solutions, but the number of random solutions for the initialization step may cause to a better result.

VI. Conclusion

Secure routing as a changeable aspect of communication is considered in this paper. the structure of various hack (as the major problems for the security) is studied and then an optimization formula base on them is designed. Multi-Objective Imperialist Competitive Algorithm is used to solve the presented formula.

References

[1] D. Rice, "A proposal for the security of Peer-to-Peer (P2P) networks: A pricing model inspired by the theory of complex networks," *IEEE.*

[2] K. Wu, T. Zhang, W. Li, and G. Ma, "Security model based on network business security," in *Proc. 2009 International Conf. on Computer Technology and Development, IEEE*, 2009.

[3] S. Hong and S. Limt, "Analysis of attack models via unified modeling language in wireless sensor networks: A survey study," *IEEE.*

[4] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *Proc. International Conf. on Devices and Communication*, 2011.

[5] X. Wang, K. R. Vishwanath, and B. Veeravalli, "Simultaneous optimization of user-centric security-conscious data storage on cloud platforms," in *Proc. 2017 IEEE 42nd Conf. on Local Computer Networks.*

[6] L. Dios, "A multi-objective evolutionary approach to the portfolio optimization problem," in *Proc. the 2005 International Conf. on Computational Intelligence for Modelling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'05)*.

[7] M. Nasir, S. Sengupta, S. Das, and P. N. Suganthan, "An improved multi-objective optimization algorithm based on fuzzy dominance for risk minimization in biometric sensor network," in *Proc. WCCI 2012 IEEE World Congress on Computational Intelligence June*, Brisbane, Australia, 2012, pp. 10-15.

[8] V. Viduto, C. Maple, W. Huang, and A. Bochenkov, *A Multi-objective Genetic Algorithm for Minimising Network Security Risk and Cost*, 2012.

[9] N. Cleetus and K. A. Dhanya, *Multi-objective Functions in Particle Swarm Optimization for Intrusion Detection*, 2014.

[10] R. M. Chintalapall and V. R. Ananthula, "M-LionWhale: Multi-objective optimization model for secure routing in mobile ad-hoc network," *IET Communications*, 2018.

[11] R. Rezaee, A. G. Bafghi, and M. Khosravi-Farmad, "A threat risk estimation model for computer network security," in *Proc. IEEE, 6th International Conference on Computer and Knowledge Engineering (ICCKE 2016)*, Ferdowsi University of Mashhad, 2016.

[12] M. H. Khyavi and M. Rahimi, "Conceptual model for security in next generation network," in *Proc. 2016 30th International Conf. on Advanced Information Networking and Applications Workshops*.

[13] Z. Lu and Y. Zhou, "The evaluation model for network security," in *Proc. 2014 Fourth International Conf. on Communication Systems and Network Technologies.*

[14] H. Ge, L. Gu, Y. Yang, and K. Liu, *An Attack Graph Based Network Security Evaluation Model for Hierarchical Network*, 2010.

[15] L. Gan, J. Liu, and X. Jin, "Agent–based energy efficient routing in sensor networks," *AAMAS'04,* New York, USA. July 19-23, 2004.

[16] W. Cheng, X. Liao, C. Shen, and S. Li, "A trust-based routing framework in energy-constrained wireless sensor networks," *WASA 2006, LNCS 4138*, pp. 478-489, 2006.

[17] X. Yao and X. Zheng, "A secure routing scheme based on multi objective optimization in wireless sensor networks," in *Proc. 2008 International Conf. on Computational Intelligence and Security*.

[18] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *ELSEVIER, Journal of Network and Computer Applications*, 2016.

[19] H. Xing, Z. Wang, T. Li, H. Li, and R. Qu, "An improved MOEA/D algorithm for multi-objective multicast routingwith network coding," *ELSEVIER, Applied Soft Computing*, 2017.

Alireza Ebrahimi Basabi received his master's degrees in software engineering from the University of of Beijing University of Post and Telecommunications (BUPT) in the China. He is currently a fourth years Ph.D student working under the supervision of professor JingSha He is in the Beijing University of Technology (BJUT). He has a background in system administration and software developer. His research interests include social media, security routing, IOT (Internet of Things), Ai (artificial intelligence), cloud computing, information assurance and network.

Jingsha He received his master's and doctoral degrees in computer engineering from the University of Maryland at College Park in the US. He is currently a professor in the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. Prior to joining BJUT in 2003, professor he worked for several multi-national companies such as IBM Corp., MCI Communications Corp. and Fujitsu Labs in the US, where he published more than 10 papers and received 12 U.S. patents. Since joining BJUT in 2003, professor He has published nearly 240 papers in journals and international conferences, received nearly 40 patents and 30 software copyrights in China and co-authored 7 books. He has been the principal investigators of more than 20 research projects. Professor He's research interests include information security, wireless networks and digital forensics.

Seyed Mahmood Hashemi get his B.Sc and M.Sc degrees from Islamic Azad University. Now, he is recent Ph.D graduate worked under the supervision of professor Jingsha He in the Beijing University of Technology (BJUT). His research interests include social media, security Routing, IOT (Internet of Things), Ai (Artificial Intelligence), cloud computing, information assurance and network.