Providing Availability in Secure Routing with Multi-Objective Model

Seyed Mahmood Hashemi
Beijing University of Technology
Chaoyang, Beijing, CHINA
Email: hashemi2138 [AT] yahoo.com

ABSTRACT---- ***Notwithstanding to the previous works on the secure routing, this paper presents a new approach base on two features: at first, presented approach is simple, so all users can understand the process of routing in the network and secondly, the given approach considers different variables independently. The primary concept of security in the presented method is 'availability,' but the used formula able to include other aspects of the network security. We use links' bandwidth and energy consuming for the route the data packets in nodes for 'availability'.***

Keywords-- Security, bandwidth, energy consuming, multi-objective model

1. INTRODUCTION

There is no doubt for the importance of security in communication via the network. Unfortunately, previous methods have two major problems: 1-used algorithms are statics and cannot adopt on the network circumstances; 2-the proposed algorithms are involved, so they need to expert users either as administrator of the network or as the costumer of the network. To fix the mentioned problems, two duties are necessary. At first, there is a need to propose a stochastic model for network security. The proposed model can cover the sudden changing in the network structure. At second, the proposed algorithm will be as comfortable as possible. Providing an approach to all aspects of the security is difficult, so in this paper, we focus on the 'availability'.

The contributions of this paper are:

- Proposing a multi-objective model for the security of the network links. The proposed model can cover multiple parameters that denote to different aspects of the security.
- I am using an evolutionary algorithm that creates a stochastic structure for the model.
- Simple vital features so that users can control it easily.

However there are some approaches to consider multiple security parameters, the conventional procedures try to assign different weights to parameters and produce a unique formula, but in the dynamic environment, such as the network that its structure deformed suddenly, assign correct coefficients as loads are difficult. In the other side, security parameters are independent of each other, so combining them into a formula cannot produce suitable results. In the proposed model, the multi-objective model considers multiple objective functions simultaneously. The concept 'availability' in the multi-objective model depends on several things, but the most important things are two: 1-bandwidth and 2-energy. If the volume of transmission data is equal or more over the bandwidth, the 'availability' disappeared. Thus to provide the security, we must make careful to the volume of the data transmission. Routing data packets consume the energy of the network nodes, and if the nodes energy be less than the satisfied threshold, then the 'availability' will be disappeared. Thus we have to consider either bandwidth and energy consuming to measuring the 'availability'.

This paper is organized as follow: in the 'Related Work' section, we study current works in this field. In part 3, we present approach and finally, in conclusion, we say about the benefits and disadvantages of the proposed method.

2. RELATED WORK

With the advent of using Wireless Sensor Network (WSN) technologies, there is a need for a new method to manage the security.

Authors of [1] claim complexity of the cyber protocols expose the network facilities to be targeted of adversaries. Some of previous studies about information security are unsuccessful, because they did not consider two key points: 1-explicit content of communication cannot limit the protection of the system, so the information security policy must include implicit information communication by "metadata"; 2-systems with stochastic structure need to security policy not just for current information, but also for the future data. Earlier systems use cryptography/encryption for security, but mention algorithms are limited to hide implicit information leakage. Continues Time Markov Chain (CTMC) is a suitable method to fix the mentioned problems of security. The principal character for the Markov process is state independence, so PrSj is independent of PrSi. The independence feature of CTMC is fully adapted to the network structure, which activation of each node is independent.

Pedro C. Pinto et al. propose a stochastic model and then introduce a secrecy rate on it [3]. Mention model needs to define a threshold, but definition threshold for different aspects of secure communication is difficult especially in changing the structure. Although their formulas, based on the Poisson distribution, are useful, they require to pre-knowledge.

Xiaohu Li et al. display system as a graph [4]. In their operations, nodes that show the system component may be secured or compromised based on the stochastic process. Authors divide security mechanism into two categories: prevention and detection.

Stephan Bohacek et al. introduce an approach for routing [5]. They use stochastic routing to minimizing computing. Although sending data packets via multiple paths is the attractive method to fix the security problem, it is not a practical method because it creates a huge overhead. Thus the proposed way in [10] is significant. Authors explore available paths base on the statistical flooding that selects hops in the random fashion. Authors of [6] propose an approach base on the port scanning.

Haihui Ge et al. propose a model to evaluate the network security base on the attack graph [7]. Their model has a risk function with three parameters: 1-asset loss, 2-threat value of attack and 3- coefficient of attack importance.

Xuanxia yao et al. suppose some parameters for secure routing [8]. The first parameter is energy that they calculate it base on the proposed formula of Long Gan et al., so if the node i wants send k bits its required energy is: Eik=Eelec.k+Eamp.k.d2 where Eelec=50njbit, Eamp=100pjbitm2 and d is distance. The second parameter is the trust ratio that they calculate it with the division the number of re-transmitted packets from node i to node j, on the number of forwarded packets base on the formula of Cheng Weifang et. al.

The biggest challenge in routing, sending the data packet from source to the final destination in the network is security, because various forms of threats and attacks cause users will feel insecure about sharing their private data in the network applications. David Airehrour et al. explore different routing protocols and their vulnerabilities [9]. They believe there are two critical 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 [10]. An example of risks of the path is transmitting a large amount of false route information to the node neighbors, to cause an overflow of a routing table. In AODV, which is routing protocol, there is a sequence number to avoid this threat [11]. However their list is useful, none of contracts can cover different risks.

Huanlai Xing et al. study was routing in the multicast manner [12]. In their paper, data is transmitted in a coding way, so they use a multi-objective evolutionary algorithm to optimize data recombination in the Network Coding based Multicast (NCM).

According to studied works, the presented approach must have the following features:

- Use multiple object functions such that functions are independent of each other.
- Stochastic structure.
- It is noting to energy consumption in the nodes.

3. PROPOSED APPROACH

Proposed security management approach includes two object functions. At first, base on the knowledge about different unavailability situations, routing data packets on the proper paths cause to the high volume of the security. A however different definition for the proper path is possible, and we focus on the bandwidth and energy consuming. In other words, more bandwidth means more properly, and also less energy consumption means more security. Bandwidth and energy consuming are independent parameters, so optimization of them must be simultaneous. Therefore the following formula presents the proposed approach:

$$\mathrm{Optimize}\ \mathrm{B},\mathrm{E}$$
$$\mathrm{B} \equiv \mathrm{Bandwidth}(\mathrm{l}_1,\mathrm{l}_2,\cdots,\mathrm{l}_\mathrm{n})$$
$$\mathrm{E} \equiv \mathrm{EnrgyConsumtion}(\mathrm{s}_1,\mathrm{s}_2,\cdots,\mathrm{s}_\mathrm{m}) \qquad (1$$

The proposed approach includes maximization of links bandwidth and minimization of sources energy consumption. If there are n links, $\{\mathrm{B_i}|\mathrm{i} \in 1,\cdots,\mathrm{n}\}$ denotes the bandwidth of links. If there are m sources of data packets, $\{\mathrm{E_j}|\mathrm{j} \in 1,\cdots,\mathrm{m}\}$

denotes the sources' energy consumption. The nodes' energy depends on two major parameters. The first parameter for energy consuming is the number of data packets. The second parameter of energy consuming is the length of the link. Thus we can write the formula for the energy consuming of the jrd as follow:

$$\mathrm{E_j = n.s.E_d} \qquad (2$$

Where n is number of data packets, $\mathrm{E_d}$ is the needed energy to transmit one data packet in link with d meter length, s is the length of link.

Suppose there is a network with 10 nodes. Each node has links to all nodes, so there are 100 links. 1 ⋯ 10 denote nodes and two nodes recognize the link between them. The following table describes the links' bandwidth.

Table 1: Link's Bandwidth

	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	n_9	n_{10}
n_1	37	15	78	74	21	69	77	61	45	76
n_2	60	43	20	62	8	62	13	31	66	39
n_3	59	78	17	2	85	97	12	91	12	5
n_4	33	7	46	93	32	95	57	10	16	26
n_5	1	46	75	8	97	31	30	3	61	73
n_6	97	74	9	58	73	40	16	38	49	92
n_7	55	20	50	31	69	85	90	3	81	60
n_8	17	58	84	5	1	54	4	32	55	80
n_9	83	6	13	3	60	59	58	30	75	95
n_{10}	89	13	38	36	53	72	17	30	90	81

The bandwidth values of links are changed over time. Another feature of the network is the length of links that the following table represents them.

Table 2: Link's Length

	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	n_9	n_{10}
n_1	72	20	83	60	24	94	4	24	32	55
n_2	71	74	87	88	14	63	86	24	21	80
n_3	24	2	38	26	7	50	39	85	5	31
n_4	15	21	60	30	62	91	95	42	29	55
n_5	19	74	74	67	64	48	19	33	71	18
n_6	72	12	37	96	38	50	30	56	70	16
n_7	38	74	15	14	70	80	45	91	65	95
n_8	94	76	98	19	30	28	32	68	68	2
n_9	83	69	7	79	55	57	28	45	33	20
n_{10}	87	16	55	62	91	34	87	11	41	71

Suppose we want to transmit 10 data packets from n1 to n10 via the network. Formula (2) calculates the energy consuming to transfer of data packets. Now, formula (1) produces a suitable path.

Table 3: Result of Proposed Approach

Suitable Path	Bandwidth	Energy
$n_1n_3 \rightarrow n_3n_2 \rightarrow n_2n_6 \rightarrow n_6n_{10}$	72	43

4. CONCLUSION

This paper presents a new method for secure routing. Although the significant target in the proposed approach is 'availability', the presented approach can develop other concepts of security. Proposed approach bases on the multi-objective optimization formula that optimizes objective functions simultaneously. The formula considers links' bandwidth and energy consuming in nodes. The significance of this paper are 1-simplicity that all network users (either administrators or clients) can understand the process of routing; 2-emphasis on variable independency.

In the next work, we can focus on other aspects of network security.

5. REFERENCES

[1] Parv Venkitasubramaniam, Parth Pradhan, "Information-Theoretic Security in Stochastic Control Systems", IEEE, Vol. 103, No. 10, October 2015

[2] Pedro C. Pinto, João Barros, Moe Z.Win," Secure Communication in Stochastic Wireless Networks—Part II: Maximum Rate and Collusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012

[3] Pedro C. Pinto, João Barros, Moe Z.Win," Secure Communication in Stochastic Wireless Networks—Part I: Connectivity", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012

[4] Xiaohu Li, Timothy Paul Parker, Shouhuai Xu, "A Stochastic Model for Quantitative Security Analyses of Networked Systems", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011

[5] Stephan Bohacek, Joa˜o P. Hespanha, Junsoo Lee, Chansook Lim, Katia Obraczka, "Game Theoretic Stochastic Routing for Fault Tolerance and Security in Computer Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 18, NO. 9, SEPTEMBER 2007

[6] VINCENT C.S. LEE, LINYI SHAO, "Estimating Potential IT Security Losses", IEEE SECURITY & PRIVACY, 2006

[7] Maochao Xu, Kristin M. Schweitzer, Raymond M. Bateman, Shouhuai Xu, "Modeling and Predicting Cyber Hacking Breaches", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 13, NO. 11, NOVEMBER 2018

[8] Haihui Ge, Lize Gu, Yixian Yang, Kewei Liu, "An Attack Graph Based Network Security Evaluation Model for Hierarchical Network", 978-1-4244-6943-7/10/$26.00 ©2010 IEEE

[9] Long Gan,Jiming Liu, Xiaolong Jin, "Agent –Based Energy Efficient Routing in Sensor Networks", AAMAS'04, July 19-23,2004,New York, USA

[10] Cheng Weifang, Liao Xiangke, Shen Changxiang, Li Shanshan, "A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks", WASA 2006, LNCS 4138,pp.478-489,2006.

[11] Xuanxia yao, Xuefeng Zheng, "A Secure Routing Scheme Based on Multi Objective Optimization in Wireless Sensor Networks", IEEE, 2008 International Conference on Computational Intelligence and Security

[12] David Airehrour, JairoGutierrez, SayanKumarRay, "Secure routing for internet of things: A survey", ELSEVIER, Journal of Network and Computer Applications, 2016

[13] Huanlai Xing, Zhaoyuan Wang, Tianrui Li, Hui Li, Rong Qu, "An improved MOEA/D algorithm for multi-objective multicast routingwith network coding", ELSEVIER, Applied Soft Computing, 2017