International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.331-340
http://dx.doi.org/10.14257/ijsia.2016.10.10.29

Study on Cybersecurity of Hybrid, Multi-hop, Wireless Network

Li Li and Hu Zhiyu

Jingdezhen University, Jingdezhen, Jiangxi, China
3172636690@qq.com

Abstract

As the frontier of Internet development, hybrid, wireless, multi-hop network has transformed the way we live. Nowadays, this network has been engaged in many areas like economy, war, culture, medical treatment, agriculture, ecology, commerce, etc. The concepts of digital coalmine and digital oilfield, in special, promote the development of the study on hybrid, wireless, multi-hop network. The paper establishes cybersecurity mechanism by introducing concepts relevant to this network, and by summarizing its internal and external security threats. By conducting simulation experiment to the security mechanism, the paper concludes that to the influence on security mechanism, the number of nodes is in direct proportion, while the transmission period of node connection in inverse proportion. The paper aims to offer reasonable suggestions and guidance to the development of hybrid, wireless, multi-hop network, to promote the application of the wireless network, and to increase its value, solve security problems and ensure sound operation of hybrid, wireless, multi-hop network.

Keywords*: hybrid, wireless, multi-hop network; cybersecurity mechanism; diffusion analysis; simulation experiment; influence relation*

1. Introduction

Science and technology are the primary productive forces, which means that the development of science, especially of computer technology, has promoted the social progress. Nowadays, low-energy wireless transmission equipment has been an emerging, potential research topic of great emphasis. And hybrid, wireless, multi-hop network has also penetrated through all aspects of people's lives. [1] Therefore, such network shall be more secure, confidential and serious. Various researches have been conducted in this area in home and abroad. University of South California studied on computing method of aggregate function on sensor network. Europe hold "Wireless Sensor Network Forum". China, with intensive and comprehensive research, also pays high attention to the development of hybrid, wireless, multi-hop network.[2]

Wire sensors, for short communication distance, are connected by routing base stations. Such connection of nodes forms wireless sensor. And the connection among wireless sensors consists of communication network, namely, hybrid, wireless, multi-hop network. This network, characterized by collectivity, universality, openness and connectivity of logic layers and physical layers, combines computer technology, wireless technology, communication technology, with information processing technology, and has different existing forms like star-network topology, mesh network topology, hybrid network topology, etc. Hybrid, wireless, multi-hop network, with extensive market prospect and high utilization value, has transformed the way we live. [3] However, restricted by the limited nodes and the objective fact that the Internet is vulnerable to attack, infiltration and leakage, the hybrid, wireless, multi-hop network is hard to conform to the security standard. Therefore, by studying on cybersecurity of hybrid, wireless, multi-hop network, the paper aims to implement secure bootstrap and security maintenance, and to optimize the allocation of resources. [4]

ISSN: 1738-9976 IJSIA

2. Security Threats Faced by Hybrid, Wireless, Multi-hop Network

Hybrid multi- hop wireless networks has been known and entered by many various types of departments in this field including enterprises, medical institutions and research institution. In early 2000s, the United States has listed the project as the first in the new technology field, and made some achievements in communication, sensing and energy calculation. European countries are also looking forward to a deepen development in this project. They are commit to study the project's issues which happened in the period of using, and made a conclusion that the problems mainly exist in the signal data sharing and the network sensor technology. There are various research activities has been carried out in Domestic about the hybrid wireless multi-hop network, mainly in the related research of sensor networks, including theoretical study cored in data and the structure rapidly changing research. They made some preliminary achievements, but at the same time, some limitations have been considered as well, such as the failure rate of network node and the limited storage capacity of computer's energy, space, computing ability, for the mixed multi-hop wireless networks have its characteristics including large quantities, high density, nodes miniaturization and finite radius and energy saving. Currently, in the situation of study, it is necessary to find the related security issues by further analysis, and to achieve the model improvement with problem solving.

2.1. External Security Threats Faced by Hybrid, Wireless, Multi-hop Network

(1) Driven by external goods like commercial interests, hackers attack system bugs by establishing malicious base stations and falsifying important network programming, which severely impedes the operation and implementation of hybrid, wireless, multi-hop network.

(2) People overestimate the coverage of hybrid, wireless, multi-hop network, namely, they believe that nodes exist everywhere. When dealing with the node scheduling, people are so idealized that they usually neglect problems like data packet dropout and energy consumption in the transmission of node diffusion. All these misconceptions lead to deviations which adversely impact the theoretical research. [5]

2.2. External Security Threats Faced by Hybrid, Wireless, Multi-hop Network

(1) Due to its hierarchical structure, hybrid, wireless, multi-hop network easily exposes to interferences from wireless environment and material distribution, to influence from hierarchical nodes collision, energy depletion and unfair competition, and to attacks like SYN flood. [6]

(2) Node perception is easily influenced by problems like shadow fading and usual faults occurring when the packets are scheduled by diffusion transmission path, that is, the node detestability is maliciously interfered. [7]

(3) When packets are transmitted in diffusion, if nodes are in frame auditory, no packets could be transmitted. [8]

(4) Due to the instability of the nodes, the nodes may change in structure or connection if it is influenced by external environment.

(5) Hybrid, wireless, multi-hop network is characterized by too many nodes and too wide node connection. And the nodes here are hard to upgrade.

(6) Energy efficiency at nodes, namely, capacity and transmission efficiency at nodes, is limited, for it is restricted by cost and physical environment.

3. Calculation Research on Hybrid, Wireless, Multi-hop Network

3.1. Essential Data of Calculation Research on Hybrid, Wireless, Multi-hop Network

Data acquisition is accomplished through video surveillance, which can be achieved by sensing and feeling, calculating and communication. Related data should be sent to each sensor receiving point and information node, and achieve the maximization of task data distribution in the space of limited resources.

3.2. Structure System of Calculation Research on Hybrid, Wireless, Multi-hop Network

Hybrid multi-hop wireless network consists of wireless network node, cluster head node and base station. The main process chart is as follows:

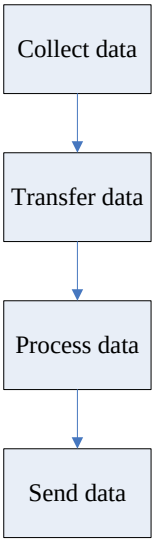

Figure 1. The Chart of Hybrid Multi-hop Wireless Network Process

Mainly it transfer the collected information and data to the sensor by the cluster head node, and the sensor will deal with these data and information according to the process for the information that can calculate easily and be used in multi-hop wireless networks. Finally, the useful information is sent to the data center for computing and storage.

3.3. Hybrid Multi-hop Wireless Network Algorithm

(1) The basic algorithm of hybrid multi-hop wireless network

It makes data to let the information does not conflict in space, even do, it also makes ellipsis processing; the information and data processing is the most important link in the whole process. But the transmission of information and data are equal without any importance ranking , and the analysis hypothesis is no priority and backward difference, for the purpose of studying the entire transmission process under the constrain time. What's more, in the process of analysis, there is a combination of dynamic and static side.

(2) Hybrid multi-hop wireless network offline algorithm

The algorithm is based on the assumption that the whole transport process is periodic and the task completion is the time of the cycle end to set the algorithm of the transmission process with full consideration of periodicity and priority. But there is limitation of the relation between the periodicity and the priority, and the actual situation is not considered.

(3) Hybrid multi-hop wireless network dynamic algorithm

Dynamic algorithm is based on the hybrid multi-hop wireless network offline algorithm, which is made by considering limitations of offline algorithm and the requirements of the current conditions.

4. The Security Mechanism Establishment Based on Hybrid Multi-hop Wireless Network

4.1. Mechanism Introduction

(1) Basic mechanism of hybrid, wireless, multi-hop network

In hybrid, wireless, multi-hop network, in cyberspace consisted of several nodes, a source node *d* is selected, with its key pool *h*, which is consisted of n keys *h*, *e*very having its corresponding key ring *j*. While every of other nodes has only one key ring *j* (the key ring becomes an identifier afterwards), and the amount of key rings at other nodes is $\sum j < n$, which means that every node has a key ring, and a key ring is shared by any two nodes. In this way, the network establishes effective, safe communication keys in connection.

(2) Multipath mechanism of hybrid, wireless, multi-hop network

Based on the basic mechanism, multipath mechanism of hybrid, wireless, multi-hop network is established for packet scheduling, because the transmission of packet diffusion may be adversely impacted by a number of connection paths between two nodes. Connection paths different in length and perception lead to various levels of cybersecurity. Cybersecurity of hybrid, wireless, multi-hop network is poor if perception and connection among nodes are simple, if the length of packet diffusion is short.

(3) Random mechanism of hybrid, wireless, multi-hop network

Random mechanism of hybrid, wireless, multi-hop network is established on the basis of multipath mechanism. In random mechanism, nodes can realize secret handshake through security certification when connecting with others. By selecting the shortest connection paths of high security, the study intends to improve cybersecurity, maintain network quality, and establish a security mechanism which is convenient and strong in secrecy.

4.2. The Assumption of the Security Mechanisms

(1) In hybrid, wireless, multi-hop network, every node at base stations has one, and only one identifier, namely, every node is unique;

(2) Hybrid, wireless, multi-hop network is free from attacks owing to its key of high security, namely, the mechanism only deals with external security threats, not with latent defect of the nodes;

(3) Semi-diameter of nodes is same in the cyberspace, namely, the speed of the transmission of packet diffusion between any two nodes is same without error. The mechanism does not cope with the influence of speed from beginning to end.

(4) Connection among nodes is not the only in the cyberspace. Every node has contiguous nodes and is connected with other nodes;

(5) Nodes do not sleep. The time of the transmission of packet diffusion can be calculated directly without regard to the influence of the notes themselves.

(6) A simulation model, which refers to the model in a certain environment, is established by only consider the verification and validation cycle, and other complex factors are not considered.

4.3. The Description of the Security Diffusion in the Mechanism

(1) Note distribution

The paper selects a node *a*, with key pool *h*, which is consisted of n keys *h*, every having one and only one identifier *j*. Identifier *j* here is formed by *Hash function*, the functional relation of relative positions of values in Hash Table. *Hash function* can be encrypted and recognized through speech. The expression is:

$$Addr = H(key) \tag{1}$$

Key is independent variable, and H is functional relation evenly distributed in Hash Table. In the expression, nodes are independent variable, and connection among nodes is functional relation.

According to node distribution and node connection in the network, the functional relation $\int$ of node distribution is:

$$\int = f(H(k_n)) \tag{2}$$

n is independent variable. $n = \{n_1, n_2, n_3, \cdots, n_i\}$, and $j = 1,2.3.4.5.\cdots, m$

(2) Gradient diffusion of nodes

The functional relation $\int$ among nodes could realize diffusion between any two nodes. Gradient here is a vector which could transmit variable, namely, a vector diffusing energy from one node to another.

For example, node d_1 with its only identifier J_1, has the functional relation $\int$ in hybrid, wireless, multi-hop network. d_1 transmits packets to the adjacent node d_2, which has only one identifier, which means that d_1 pairs with d_2.

Case 1: Nodes can exchange information, transmit packets and realize connection if they share the same key *w*, as shown in the following figure.

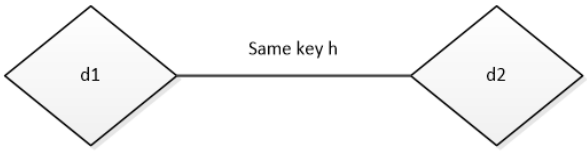

Figure 2. Successful Connection between Two Nodes

Case 2: If node d_1 cannot pair with node d_2 because they do not share the same key h, d_1 will pair with the next node d_3, as shown in the following figure.

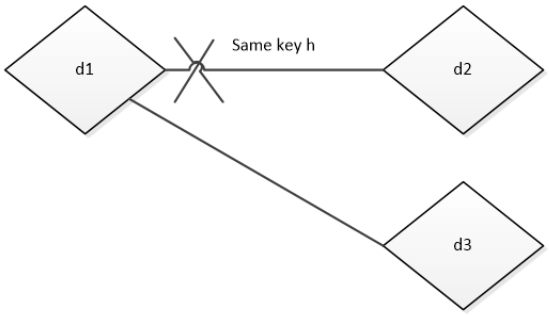

Figure 3. Failing Connection between Two Nodes

As mentioned above, any node pairs with its adjacent nodes one by one until finding the node with the same identifier, after that the node can connect with the one with the same identifier. In hybrid, wireless, multi-hop network, all nodes can successfully pair and connect with the others, and the connection paths spread across the cyberspace, as shown in the following figure.

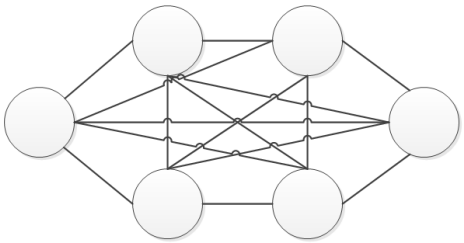

Figure 4. Connection among Nodes

4.4. The Analysis of Security Mechanism of Hybrid, Wireless, Multi-hop Network

Given the latent defects of the nodes, this part analyses the security mechanism of hybrid, wireless, multi-hop network. In such network, data leakage exists in the transmission between nodes, for example, node d transmits packets to node e after connection, and then e connects with the adjacent node f, transmitting packet to it. After that transmission, data at e may suffer leakage. In this process, d reaches an agreement of data leakage with f in advance. Data leakage between nodes happens in this way.

Figure 5. Data Leakage between Nodes

The paper established the security mechanism of hybrid, wireless, multi-hop network in order to reduce or avoid data leakage. Frequency counter is set at every node to calculate the times of receiving packets. The counter displays "1" when the node receives packet at the first time, and the like. When the statistics of reception p is greater than that of transmission q, the risk of data leakage is high and the mechanism is not credible. On the contrary, when the statistics of reception p is less than that of transmission q, the risk of data leakage is low and the mechanism is credible. Transmission period T exists in the transmission of packet diffusion. When the period is long, the cost of communication is high and the life cycle of hybrid, wireless, multi-hop network is short. On the contrary, when the period is short, the cost of communication is low and the life cycle of hybrid, wireless, multi-hop network is long.

The paper supposes that there is a leakage node with statistics O and an identifying statistics T which indicates that data is leaked after transmitting among T nodes. If the identifying statistics is greater than the leakage statistics, namely, $T > O$, the mechanism can detect all nodes which have reached an agreement of data leakage. On the contrary, if the identifying statistics is less than the leakage statistics, namely, $T < O$, the mechanism can not detect all nodes which have reached an agreement of data leakage.

$$z = {q+1}\big/{p+2} \tag{3}$$

If the statistics of packet reception of node d is p, and that of d's nearest node e is q, and the trust value of d to e is z, it can be summarized that:

In hybrid, wireless, multi-hop network, nodes exchange statistics of packet transmission to other connected nodes regularly. Any node identifies connections by identifying statistics T. And it begins to identify connection with the nearest node. If the node cannot receive statistics from its neighbor, it will not upload information to the adjacent one for the low credibility and the possibility of data leakage. But if the node can receive statistics from its neighbor normally, it will identify the next node, until all nodes in the cyberspace are identified.

5. Simulation Experiment

With the characteristics of low cost, wide range of benefit and high quality resources, virtual simulation experiment, by complying with the requirements of the development trend in modern education and teaching, has practiced teaching means and established a background of verification conditions on the basis of computer and multimedia equipment to conduct the simulation experiments on the model and mechanism which effectively promoted the deepening of information management and has a positive and significant influence on the reformation of information quality, and strengthen the guidance and normative of information construction as well. What's more, it is conducive to the sharing of high quality information resource promotion and to provide the advanced management concepts and construction experience of the related fields.

The paper studied on the security mechanism of hybrid, wireless, multi-hop network by using simulation software of discrete event in the Internet. The hierarchical structure established by the simulation software is as follows:

As shown in the figure, the hierarchical structure starting from an origin node is consisted of k layers every of which has three nodes and one leakage node. And the speed of packet transmission is $100/k$.

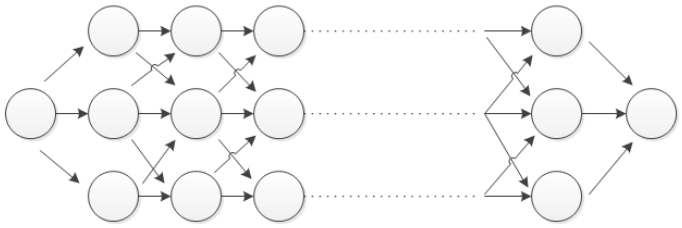

Figure 6. Simulation Experiment Mechanism of Hybrid, Wireless, Multi-hop Network

In view of packet dropout, simulation software connect each two adjacent nodes on the premise of regulated node radius and packet transmission speed. The experiment aims to prove the influence of identifying statistics and identifying period to the security mechanism.

5.1. Influence of Identifying Statistics on the Security Mechanism

The influence of identifying statistics on the security mechanism in hybrid, wireless, multi-hop network enhances with the increase of identifying statistics.

The bigger the reception statistic is, the larger the influence on hybrid multi-hop wireless network is. And the influence is stable after the reception statistics increases to a certain level.

5.2. Influence on Identifying Statistics to the Security Mechanism

As shown in the figure, the influence on the security mechanism decreases with the increase of identifying period. And the influence is becoming stable in spite of the sharp grade after the transmission period decreases to a certain level.

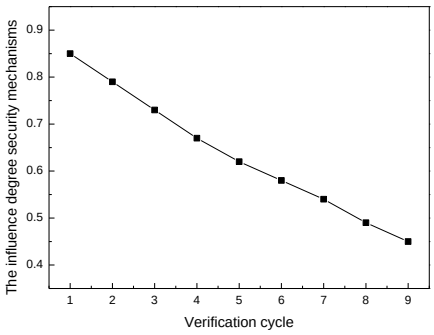

Figure 7. Influence on Identifying Statistics to the Security Mechanism

The longer the node connection time is, the weaker the influence on hybrid, wireless, multi-hop network is. And the influence also decreases with the increase of reception statistics. In long terms, the influence on security mechanism decreases linearly with the increase of the transmission period (time of nodes connecting with others). And the influence is becoming stable after the transmission period increases to a certain level.

6. Conclusion

Hybrid, wireless, multi-hop network enjoys great momentum in today's society, and can be utilized in all aspects of life. By conducting simulation experiment to the security mechanism, the paper concludes that (1) the influence of identifying statistics on the security mechanism enhances with the increase of identifying statistics and remains stable after the reception statistics increases to a certain level; (2) the influence on the security mechanism decreases with the increase of identifying period and remains stable after the reception statistics increases to a certain level. Based on this conclusion, people can not only reduce the time of node connection, but improve the security of network. In brief, the paper is of guiding significance in future research on hybrid, wireless, multi-hop.

Future Development Advice

With the wide application of electronic and computer technology, the hybrid multi-hop wireless networks have already become the hot trend and priority in people's eyes.

(1) Fully considering the real situation of the hybrid wireless multi-hop network which has the characteristics of complexity diversity, comprehensiveness and variability, in order to deal with complex situation, this network should upgrade based on the existing hybrid wireless multi-hop network mechanism through the introduction of multiple variables.

(2) Subjective and objective connection. The establishment of the mechanism and model not only consider the external environment, but also consider the human factor. According to the needs of humanity, to build and apply.

(3) Considering the energy limitation of hybrid wireless multi-hop networks. Energy issues directly affect the capacity of the network space, and to solve the node problem and the connection of hybrid multi-hop wireless networks has become the most important part.

(4) To clean up the redundant information. In the process of connection between information nodes, the information rubbish will be accumulated, which makes the original limited space become narrower and affecting the normal data connection.

(5) For the personnel problems of accidental and blind area of hybrid multi-hop wireless network needs to further improve the model in practical application and research, by narrowing the communication radius of node information, to realize the coherence of the whole network data transmission and connectivity.

(6) Cross layer design makes all levels of construction boundary fuzzy in hybrid multi-hop wireless network, which has beneficial effect high level agreement is not affected by the low level physical layer transmission. According to the network characteristics and the research on the security mechanism of the application scenarios, you can improve the performance of hierarchical network.

(7) Considering the scalability problem and the capacity of each level of the wireless multi-hop network adjustment problems, in-depth study and improve the link between media, network support and network layer security.

This paper just preliminary study, future work will relates to more factors, wider range, and more complex environment. The development of hybrid multi-hop wireless network must be enforced, and it also has become a dynamic motivation to promote and deepen the development of the project with the background of rapidly forward today in computer, electronic communication and network.

References

[1] J.-H. Cui, J. Kong, M. Gerla and S. Zhou, "Challenges: building scalableand distributed underwater wireless sensor networks (UWSNs) for aquatic applications", IEEE Network, Special Issue on Wireless Sensor Networking, vol. 20, **(2006)**, pp. 12-18.

[2] D. Pompili, T. Melodia and I. F. Akyildiz, "Three-dimensional and two-dimensional deployment analysis for underwater acoustic sensor networks", Ad Hoc Networks, vol. 7, **(2009)**, pp. 778–790.

[3] M. D. Hatch, J. L. Kaina, M. Owen, R. P. Mahler, R. S. Myre and S. J. Benkoski, "Data Fusion Methodologies in the Deployable Autonomous Distributed Systems Project", In: 1998 International Conference on Multisoure-Multisensor Data Fusion. Las Vegas: International Conference on Multisoure-Multisensor Data Fusion, **(1998)**, pp. 470-477.

[4] J. A. Rice, "Enabling Undersea ForceNet with Seaweb Acoustic Networks", Biennial Review 2003. San Diego: SSC San Diego, **(2003)**, pp. 174-180.

[5] J. Rice, "Underwater Acoustic Communications and Networks for the US Navy's Seaweb Program", In: 2008 Second International Conference on Sensor Technologies and Applications. Cap Esterel, France: International Conference on Sensor Technologies and Applications, **(2008)**, pp. 715-722.

[6] J. Rice, "SeaWeb Acoustic Communication AND Navigation Networks", In: Proceeding of the International Conference Underwater Acoustic Measurements: Technologies & Results. Heraklion, Crete, Greece: International Conference Underwater Acoustic Measurements, **(2005)**, pp. 1-7.

[7] Rice J., Creber B., Fletcher C., Baxley P., Rogers K., McDonald K., Rees D., Wolf M., Merriam S., Mehio R., Proakis J., Scussel K., Porta D., Baker J., Hardiman J. and Green D., "Evolution of Sea Web Underwater Acoustic Networking", In: Oceans 2000 Conference. Providence, RI, USA: Oceans, **(2000)**, pp. 2007-2017.

[8] J. A. Rice, "Undersea Networked Acoustic Communication and Navigation for Autonomous Mine-Countermeasure Systems", In: 5th International Symposium on Technology and the Mine Problem. Monterry, CA: International Symposium on Technology and the Mine Problem, **(2002)**, pp. 1-9.

[9] V. Chandrasekhar and Y. S. Choo, "How Voon Ee. Localization in Underwater Sensor Networks−Survey and Challenges", In: WUWNet '06 Proceedings of the 1st ACM International Workshop on Underwater Networks. Los Angeles, California, USA: the 1st ACM International Workshop on Underwater Networks, **(2006)**, pp. 33-40.

[10] J. G. Proakis, E. M. Sozer, J. A. Rice and M. Stojanovic, "Shallow Water Acoustic Networks", IEEE communications Magazine, vol. 39, no. 11, **(2001)**, pp. 114-119.

Authors

Li Li, she was born in Jingde, Jiangxi province in the December of 1983, she is a lecturer of the JingDe Institute, her research direction is computer network technology and software engineering.

Hu Zhiyu, he was born in , Yi County, Anhui province in the March of 1983, is a lecturer of the Jingde Institute, his research direction is graphics, artificial intelligence and computer network.