Research Article

HUMAN SAFETY AND SECURE TRUST MANAGEMENT SCHEMES FOR UNDERWATER WIRELESS SENSOR NETWORKS

Porkodi K.P.*, A.M.J. Md. Zubair Rahman

Department of Computer Science and Engineering, Al-Ameen Engineering college, Erode, Tamil Nadu, India

*Corresponding Author Email: porkodiprabhakaran@gmail.com

Article Received on: 15/04/17 Approved for publication: 25/05/17

DOI: 10.7897/2230-8407.08585

ABSTRACT

A trust management scheme is a new technology for underwater wireless sensor networks. The increasing deployments of sensor nodes and dynamic network topology have not been utilized properly due to some of poor controlling mechanism and safety of mobile sensor nodes. The proposed safety and sensor trust cloud management will explain in this paper how safely and securely the trust management is implemented in underwater wireless sensor networks. This method will help all the human beings to protect from electromagnetic ways, and it will increase the human and animal life's and reduces the cost of paramedical since the communication is taken in underwater. The SSTMC are compared with existing trust management mechanism and it will conclude how the humans and animals are prevent from the electromagnetic ways.

Keywords: WSN, UWSNS, TCM, SSTMC

INTRODUCTION

In the recent years, the underwater wireless sensor networks (UWSNS) has plays a vital role in research due to their rapid application development in many different areas such as ocean graphic data collection, marine environment monitoring, ocean logical surveillance, underwater assisted navigation, disaster forecast and prevention etc., In the underwater wireless sensor nodes communication, partnership of sensor nodes are very essential. So the malicious attackers can seriously threaten the communication operation of UWSNS. The efficiency of underwater wireless sensor networks is implemented through the secure communication and association among several nodes^{1,2}. For implementing the secure communication, there have been 3 kinds of security mechanisms available.,

- Intrusion protection system
- Intrusion detection system
- Intrusion tolerance system

Intrusion tolerance is considered to be a best security mechanism. In the current era many new algorithms implements intrusion tolerance mechanisms for the best security such as internet, terrestrial WSN(TWSN), point-to-point(p2p)networks, ad-hoc networks, TCM social networks and so on. For further improve the network security and trust management and malicious this SSTCM also implements intrusion tolerance system.

The functional requirement of trust mechanism is differ from each and every application. Due to the unique characteristics of the underwater environment and acoustic communication the existing wireless sensor networks trust mechanism cannot apply directly in the underwater communication. so a new algorithm with fuzziness and randomness logic named as TCM (Trust Cloud Model) was implemented according to the communication behaviors of the nodes in cloud environment

the trust calculation is made by direct trust cloud establishment, recommendation trust cloud establishment and indirect trust cloud establishment. by Applying any one of these method to reach the destination path but the method has faces lot of difficulties for trust assessment due to position of sensor nodes or lack of identification of nodes and it is difficult to face large scale environment¹. so to implement the large scale environment and trust assessment. We have proposed an algorithm named as a human safety and secure test management schemes for underwater wireless sensor networks (SSTMC).

In this paper Section II will discuss about the existing trust management intrusion tolerance mechanisms. Section III will describe about the performance of our proposed Fulkerson's rule implementation of safety and secure trust management scheme for underwater wireless sensor networks. Section IV describes the performance of network. Section V concludes the paper.

RELATED WORK

This section will explore about the existing trust management schemes. Since the trust management has given more privileges to identify the malicious nodes and the work of the trust management starts from collecting trust evidence according to the behavior of the sensor nodes and it applies mathematical methods to check whether the node is useful or not³. According to the mechanism and mathematical model in wireless sensor networks the trust management can be divided in to several categories. In that we can we reviewed some of the important model which was applied in WSN.

Reputation-Based Framework For High Integrity Sensor Networks (RFSN)

RFSN is the first trust concept in WSN. It is based on Bayesian theory names as REPUTATION –BASED FRAME WORK

FOR HIGH INTEGRITY SENSOR NETWORKS and it is the most used trust mechanism in wireless sensor networks. But it is efficiently focused only for successful or unsuccessful communication⁴. To evaluate these trust in UWSN is not reliable because the UWSN communication easily interrupted by the environment.

Trust Management Based On Probability Theory

A trust management by using probability theory was implemented as follows. In the first step through a basic statistical method the relevant trust factor are obtained. Then the sensor nodes trust values are calculated by the weighted algorithm⁵. In addition it is very hard to accurately obtain trust evaluation method in UWSN because it is difficult to find the proper size of each weight value in UWSNS.

Trust Management Based On D-S Evidence Theory

Feng introduced a D-S evidence theory where it will directly say "inaccuracy" and "uncertainty". However, the computation complexity is high in D-S evidence theory and increases in the exponential order 6. The drawback is when the number of nodes is increased it is very difficult to implement the exponential order.

Trust Management Based On Fuzzy Logic

To overcome the drawbacks of probability and Bayesian theory Chen and groups studied the fuzzy logic and the inference rule is established to implement the fuzziness and it cannot provide a specific quantitative method for trust value⁷. Due to the above rule it cannot be suit in UWSNS.

Trust Management Based On Entropy And Recommendation Chain Classification Theory

To overcome the problem of adhoc entropy theory⁸ and TWSN entropy theory⁹. Zhang proposed a trust model focuses on entropy and recommendation chain classification¹⁰. As compare with the traditional subjective model trust management mechanisms based on entropy theory can get correct trust evaluation.

Trust Management Mechanism Based On Cloud Theory

In 2009, Mr. B. MA. introduced a trust cloud into TWSNS and put forward a cloud-based trust model (CBTM). In addition, using the average method to evaluate trust values of sensor nodes is not reasonable¹³. In 2014, X.XU team designed a light weight cloud model for TWSN¹². As analyzed with the above Trust cloud model can't apply directly in the UWSNS.

Trust Cloud Model In UWSNS

TCM (TRUST CLOUD MODEL) introduce a trust model based on cloud theory in UWSNS. In this article, the mathematical cloud concept was described the uncertainty qualitative and quantitative very well. But the communication behaviors and trust relationships between sensor nodes will constantly change which makes the trust evidence in confusion stage¹¹. In the above method there is a possibility that same node can be used more than once. So, the uniqueness is less.

MATERIALS AND METHODS

FULKERSON'S RULE IMPLEMENTATION

To improve the trust evidence and the accuracy of information exchange and node uniqueness is implemented by Fulkerson's rule.

The Fulkerson's Numbering rule is implemented in the following manner:

STEP1: In our cloud environment, at the initial stage all the sensor nodes are trust worthy, since there is no past communication mark any node as initial node and number it as 1.

STEP2: In the second step, if it is many nodes are available for communication, delete all neighborhoods nodes and find the new node based any one of the TCM methods¹¹. This will create at least one new initial event.

STEP3: Number these initial event as 2,3,.

STEP4: Delete the leaving arrows from the numbered events, which will, in turn produce new initial events and then follow step3

STEP5: Continue the process until the destination node is obtained which has no arrows

RESULT AND DISCUSSION

The implementation of Fulkerson's with diagram is explained below

Figure 1: Randomly Deployed Sensor Nodes in the Cloud Environment.

Figure 1 shows the randomly deployed sensor nodes n in the cloud environment

Figure 2: Initial node mark by using Fulkerson's algorithm

Step1:

In our network, at the initial stage all the sensor nodes are trust worthy, since there is no past communication mark any node as initial node and number it as 1. (Figure 2)

Figure 3: Finding next node by Fulkerson's algorithm

Step2 &3:

If it is many nodes are available for communication, delete all neighborhoods nodes and find the new node based any one of the TCM methods. This will create at least one new initial event. Figure 3

This process will continue until the node has to reach the destination node

Figure 4: Final output

Step N:

Based on the FULKERSON'S Numbering rule implementation approximate output is shown in the Figure 4.

Figure 5: The comparison of successful communication rate with TCM and SSTCM

The Performance of Data Transmission

As compare with the TCM model the SAFETY AND SECURE TRUST MANAGEMENT SCHEMES FOR UNDERWATER WIRELESS SENSOR NETWORKS rate with the increasing number of malicious nodes. The SSTCM method provides a secure and confidential way to reach the destination path and it

is used to monitor the large scale node. The SSTCM method will reduce the trust assessment difficulties. The position of the node can be identified by the numbering so when the sensor nodes changes with ocean flow, the numbering method will help to identify the past communication and if the communication is far away the secure and safety method is used to give the information details in a secure way to develop trust relationship. The Figure 5 shows the comparison of successful communication rate with TCM AND SSTMC

CONCLUSION

In this article, we have described and compared with existing cloud model with WSN (Wireless sensor networks) and UWSN and the SSTMC will increases communication behavior of trust relations ship between sensor nodes. This method will help all the human beings to protect from electromagnetic ways, and it will reduce the cost of medical expenses. Since the communication is taken in underwater. Through this SSTCM method the malicious attacks is very low because all the nodes are tightly coupled with application process.

But there are still many challenges remaining for future challenges:

Poor stability of underwater communication
Limited to explore in the real time world

Acknowledgement

I am very thankful to the institute Al-Ameen engineering college for providing the valuable support to undergo research.

REFERENCES

1. Guangjie Han, Jinfang Jiang, Ning Sun, Lei Shu. Secure communication for underwater acoustic sensor network. Institute of Electrical and Electrical Engineering Communications Magazine. 2015; 53 (8): 54 – 60.
2. Guangjie Han, Jinfang Jiang, Lei Shu, Mohsen Guizani. An Attack-Resistant Trust Model Based on Multidimensional Trust Metrics in Underwater Acoustic Sensor Network. Institute of Electrical and Electrical Engineering Transactions on Mobile Computing. 2015;14(12), 2447 – 2459.
3. Guangjie Han, Jinfang Jiang, Na Bao, Liangtian Wan, Mohsen Guizani. Routing protocols for underwater wireless sensor networks. Institute of Electrical and Electrical Engineering Communications Magazine. 2015; 53 (11), 72 – 78.
4. Ganeriwal S, Balzan LK, Srivastava MB. Reputation based framework for high integrity sensor networks. Association for Computing Machinery Transactions on Sensor Networks. 2004; 66–77.
5. Crosby GV, Pissinou N, Gadze J. A framework for trust-based cluster head election in wireless sensor networks. Second Institute of Electrical and Electrical Engineering Workshop on Dependability and Security in Sensor Networks and Systems. 2006;: 10 – 22.
6. Chen Chao, Wang Ru-chuan, Zhang Lin. The Research of subjective trust model based on fuzzy theory. In open Networks. Acta Electronica Sinica. 2010; 11: 2505-2509.
7. Renjian Feng, Xiaofeng Xu, Xiang Zhou, Jiangwen Wan. A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory. Sensors. 2011; 11(2): 1345-1360.
8. Yan Lindsay Sun, Wei Yu, Zhu Han, Liu KJR. Information theoretic framework of trust modeling and evaluation for ad hoc networks. Institute of Electrical and Electrical

- Engineering Journal on Selected Areas in Communications. 2006; 24 (2): 305 – 317.
9. Dai Hongjun, Jia Zhiping, Dong Xiaona. An entropy-based trust modeling and evaluation for wireless sensor networks. 2008 International Conference on Embedded Software and Systems. 2008; 27 – 34.
 10. Zhang Lin, Xing Huan, WANG Ru-chuan, WU Chao-jie L. Dynamic trust model based on recommendation chain classification in complex network environment. Journal on communications. 2015; 36 (9): 55–64.
 11. X. Xu et al. Representation for Uncertainty Trust of WSN Based on Lightweight-Cloud. Journal on communication. 2014; 35 (2): 63–69.
 12. Jinfang Jiang, Guangjie Han, Chunsheng Zhu, Sammy Chan, Joel J. P. C. Rodrigues. A Trust Cloud Model for Underwater Wireless Sensor Networks. Institute of Electrical and Electrical Engineering Communications Magazine. 2017; 55 (3): 110 – 116.
 13. Bin Ma. Cross-Layer Trust Model and Algorithm of Node Selection in Wireless Sensor Networks. International Conference on Communication Software and Networks. 2009; 812–815.

Cite this article as:

Porkodi K.P. and A.M.J. Md. Zubair Rahman. Human safety and secure trust management schemes for underwater wireless sensor networks. *Int. Res. J. Pharm.* 2017;8(5):120-123
<http://dx.doi.org/10.7897/2230-8407.08585>

Source of support: Nil, Conflict of interest: None Declared

Disclaimer: IRJP is solely owned by Moksha Publishing House - A non-profit publishing house, dedicated to publish quality research, while every effort has been taken to verify the accuracy of the content published in our Journal. IRJP cannot accept any responsibility or liability for the site content and articles published. The views expressed in articles by our contributing authors are not necessarily those of IRJP editor or editorial board members.