International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

A Novel Optimal Routing Protocol for Wireless Ad hoc Network with the aid of Double Encryption Mechanism

Pratibha Kantanavar

Abstract: ***Ad hoc network paved way to various researches and application due to its wide acceptance over wired network. The advance has also led to various drawbacks or problems that can result in unauthorized usage of data or in data loss. So secured data transfer has become an important requirement in any Ad hoc network. Various issues exist in Ad hoc network while data transmission and hence it has become a major requirement to develop an efficient routing protocol that can transmit the data securely over the network. So, this paper provides a solution, intend to develop an approach for making the data transmission more secured and feasible. This paper incorporates double encryption scheme to secure the data where we use Hybrid DNA based cryptosystem and blow fish algorithm for authentication of users. Also, we design an efficient optimal routing protocol that makes the transmission secured by reducing various attacks that occur in the network. It provides the security for image transmission over internet effectively. This technique also can be extended in multimedia security over the internet. The network parameters will be approximately judged in order to demonstrate the performance of the scheme we develop.***

Keywords**:** ***Geo-Location Oriented Routing (GLOR), Secure-GLOR***

I. INTRODUCTION

Recently, the wireless technology was found to be one of the significantly deployed networking technologies due to its capabilities and numerous advantages. The proliferation of this technology has led to the growth of wireless ad hoc networks and was found to be used in several applications of wireless sensor networks in both civilian and industrial applications (Firdhous, 2016). The working of these networks was based on a group of wireless mobile nodes which mutually exchanges the data within themselves without any centralized administration or fixed base station. The characteristics of these wireless ad hoc networks were found to provide support in extreme situations such as rescue, and emergency operations (Lu et al.,2016).

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
Pratibha Kantanavar*, Department of Electronics & Communication Engineering, RV College of Engineering, Bengaluru. Karnataka, India. Email: pratibhakantanavar@rvce.edu.in

The performance of wireless ad hoc was found to be related to the reliable routing within the nodes and the data transmission is performed with the assistance of neighboring nodes of the system (Cho et al.,2011).

In recent past, extensive studies were conducted on the routing manners involved in wireless ad hoc networks, and this has resulted in several novel routing protocols. Besides, the major limitations observed in these routing protocols were such that these systems were designed with an assumption that all nodes involved were fully trusted and Cooperated with each other (Jawandhiya et al.,2010).

However, several researches suggest that these nodes were vulnerable to malicious nodes that were found to disobey the routing regulations.

In addition, the reliability of these protocols was found to be depended on several factors such as the nature in which the transmission occurs, fixed infrastructure and the challenging topology (Baburajan et al.,2014).

These, parameters were found to influence the design of reliable protocols in wireless ad-hoc networks and making it more challenging. The understanding of distinct routing attacks is necessary to design an effective prevention mechanism that is required to achieve reliable routing attacks. Further, perception of the characteristics of the attacker during the routing process is needed to develop appropriate security mechanisms. Several literatures were found to provide the details regarding the classification of routing attacks.

The surveys were found to express diverse types of attacks involved in the routing mechanisms such as routing loop, wormhole, and black hole (Nakul, 2013).

The analysis of different attacks on the routing mechanisms were found to comprise of two dimensions in which the first dimension is related to the attacker who was found to misuse the routing message while the second dimension is based on the objectives perceived by the attackers (Lim et al.,2013).

Furthermore, the deployment of these networks in open space and the constraints in the nodes for numerous applications was found to be vulnerable to several security threats.

The unique nature of these wireless adhoc networks were found to limit the implementation of security mechanism and algorithms designed for the traditional networks. Thus, active research is necessary to be conducted worldwide for creating a more secure, reliable and user friendly wireless networks.

II. ENCRYPTION TECHNIQUES

A. Significance of Double encryption technique

Presently, several techniques have been carried out for the implementation of encryption in data to ensure the data security in a wireless sensor network based on specific criteria. However, it was noticed that for an effective encryption it is necessary to have an appropriate distribution and management system.

Besides, the involvement of external sources was found to influence the wireless networks and thus limiting the use of conventional management schemes in the wireless networks (Virmani et al.,2014). In addition, the resource constraints in sensor networks was also found to restrict the use of existing algorithms and defense mechanisms in the wireless ad-hoc network. Hence, from this research work the requisite for the development of efficient the cryptographic schemes that needs to be employed in a wireless sensor network can be observed. Furthermore, code, data size, required time for processing and power consumption need to be considered while developing the schemes (Dogra and Kohli, 2016).

In addition, implementation of cryptography was found to be very expensive and thus was found to be limited in the use of wireless ad-hoc networks.

Therefore, several researches have been conducted to develop a symmetric key for the cryptography such that it could be used in constrained systems.

However, the major drawback found in this research was in terms of the key management as the symmetric key was found to utilized for both encryption as well as decryption. Besides, it is significant to assign the key to the receiver confidentially.

The major shortcomings observed in this research was concerned with single point of failure and scalability (Li et al.,2017).

Moreover, a secure version of the Geo-Location Oriented Routing (GLOR) protocol was postulated for assimilating the security framework in wireless mesh networks. This study was found to incorporate several features involved in the network model and further enables encryption in order to provide a high level of security throughout the network. However, from this research it was observed that as the size of the data set increases the computation time and resources that is required to perform the task also increase while implementing the asymmetric encryption techniques (Nanda et al.,2017).

From the above studies the requirement to develop a novel protocol considering the size of data, computation time, cryptography key to ensure data security and reliability within the wireless ad-hoc networks is observed.

B. Objectives

This paper focus here on three objectives:

1.To determine the mechanisms by which malicious nodes disobeys the routing regulations.

To develop a novel optimal routing protocol for a reliable wireless ad-hoc network with the aid of double encryption mechanism

2.To establish a secure and low power consumption routing protocol.

III. RESEARCH METHODOLOGY

This study will develop an efficient methodology to ascertain the security measures in order to protect the wireless ad-hoc networks from heterogeneous attacks. In this study, initially the behavior executed by the attackers will be analyzed to develop a trust-based routing protocol. In addition, the existing AODV routing protocols of wireless ad-hoc network were found to be exploited by the attackers. T

hus, the deficiencies of the conventional protocols will be realized to develop an efficient defense mechanism against the attackers to ensure the data security.

Furthermore, Geo Location Oriented Routing (GLOR) was postulated in the previous studies as a hybrid routing protocol which was designed to support large, dynamic networks such that there is no compromise on the reliability and security of the network and the devices related.

The DNA cryptography approach was found to be emerging as a promising approach in the development of defense mechanisms in wireless network.

Thus, this research will develop a cryptographically secure communication protocol by integrating the Geo Location Oriented Routing (GLOR) based on a Hybrid DNA-based Cryptography (HDC).

This technology will be employed for sophisticated wireless ad-hoc network as it will require lesser computational power, bandwidth and memory. The steps involved in the methodology of the proposed method are described as follows:

A. Stage1

1.Node Addressing

This stage determines the instantaneous position of each node by using GPS and addresses the location of the nodes. Detailed process shown in Fig 1.

2.Data Packets

The packet header will be designed to contain the required information's to calculate the path in order to carry more data and reduce the overhead. Packet transmission is in store and forward manner through wireless multi hop connection. Packet consists of source n destination node identification and other information related to routing.

As the size of packets increases means data contains in packet increases and overhead bits reduces. Real time video or any multimedia data transmission in wireless environment is noisy and data loss is unavoidable. So need to retransmit the corrupted packets.

When packet size is more, it will affect throughput, delay and data dropped. We can apply proactive routing protocol OLSR (Optimized link state routing). It shows less delay but packet fragmentation has to be taken care. Small packet size consideration gives better throughput and very less delay for real time application.

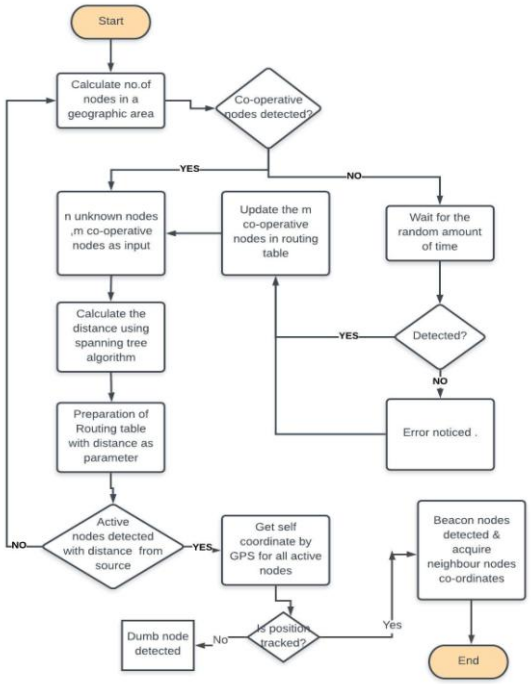

Fig 1: Node addressing using geographic forwarding

B. Stage 2

This model is developed by focusing the authentication and encryption aspects of routing and is implemented through different network levels. In the authentication stage the data is initially analyzed by the authenticated node and is compared with the data collected by its neighboring nodes from the device. Thus, further analysis is performed by the web register and monitors the network conducted by the web register.

The asymmetric encryption throughout the network is used to secure the data transmitted through the nodes. As the node is authenticated, the data transmitted through the node will be encrypted. The encryption technique used in this research is RSA algorithm. This process is defined as a DNA assembled public key encryption scheme that provides an effective storage method of cipher text and public key in the DNA strand. Furthermore, this system provides double encryption which was found to be difficult for adversary to break the cryptosystem.

C. Stage 3

The integrity of the data is verified and authenticated by employing hybrid DNA based cryptosystem by utilizing both the public and private key-based schemes. Thus, integrity and confidentiality will be achieved by symmetric encryption while the node authentication will be performed by asymmetric encryption.

Therefore, the implementation of this research work will provide enhanced security, less overhead computation and better performances of wireless ad-hoc network.

IV. CONCLUSION

The node addressing in WANET will be determined by Spanning tree & GPS localization algorithms. Once the node addressing has been determined, the designing of data packets is done by fragmenting larger data packets into smaller ones. Then, the smaller data packets are transmitted to their destination using OLSR algorithm. Finally, the double encryption is achieved by applying double encryption model to these transmitted data packets using Hybrid DNA algorithm.

This paper will provide a safe and seamless performance of the wireless ad-hoc networks by finding a universal solution for the emerging routing attacks. In addition, this research also considers numerous factors such as key management, cryptography and diverse security techniques to ensure secure routing protocol which will minimize the security impact on the network in order to deliver an acceptable network performance of a wireless data network.

REFERENCES

1. Firdhous, M. F. M. (2016). Security Implementations in Smart Sensor Networks. In Trends in Ambient Intelligent Systems (pp. 187-221). Springer International Publishing.
2. Lu, X., Wang, P., Niyato, D., Kim, D. I., & Han, Z. (2016). Wireless charging technologies: Fundamentals, standards, and network applications. IEEE Communications Surveys & Tutorials, 18(2), 1413-1452.
3. Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 13(4), 562-583.
4. Jawandhiya, P. M., Ghonge, M. M., Ali, M. S., & Deshpande, J. S. (2010). A survey of mobile ad hoc network attacks. International Journal of Engineering Science and Technology, 2(9), 4063-4071.
5. Baburajan, J., Prajapati, J. (2014). A review paper on watchdog mechanism in wireless sensor network to eliminate false malicious node detection. Int. J. Res. Eng. Technol. 3(1), 381–384
6. Nakul, P. (2013). A survey on malicious node detection in wireless sensor networks. Int. J. Sci. Res. 2 (1), 691–694
7. Dogra, H., & Kohli, J. (2016). Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey. Indian Journal of Science and Technology, 9(47).
8. Li, S., & Da Xu, L. (2017). Security in Enabling Technologies. Securing the Internet of Things, 109.
9. Nanda, A., Nanda, P., He, X., Jamdagni, A., & Puthal, D. (2017, August). Secure-GLOR: An Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks. In Trustcom/BigDataSE/ICESS, 2017 IEEE (pp. 269-276). IEEE.
10. Li, W.T., Feng, T.H., Hwang, M.S. (2014). Distributed detecting node replication attacks in wireless sensor networks: a survey. Int. J. Netw. Secur. 16(5), 323–330
11. Virmani, D., Hemrajani, M., Chandel, S. (2014). Exponential trust based mechanism to detect black hole attack in wireless sensor network. Int. J. Soft Comput. Eng. 4(1), 14–16
12. Lim, S.Y., Choi, Y.H. (2013). Malicious node detection using dual threshold in wireless sensor networks. J. Sens. Actuator Netw. 2, 70–84

AUTHORS PROFILE

Pratibha Kantanavar received B.E degree in Electronics & Communication Engineering from VTU,Belagavi in 2010. M.Tech degree in communication systems from VTU Belagavi in 2012.

She is working in the department of Electronics & Communication Engineering of RV College of Engineering, Bengaluru. She has 4 years of teaching experience; she has published 4 research papers in International journals. She has attended 7 seminars and workshops. Her area of interests is network security, MANETs, VANETs and IoT applications.