6

Contents lists available at ScienceDirect

International Journal of Intelligent Networks

KeAi
CHINESE ROOTS
GLOBAL IMPACT

SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks

K. Vinoth Kumar [a, *], T. Jayasankar [b], V. Eswaramoorthy [c], V. Nivedhitha [c]

[a] Department of Electronics and Communication Engineering, SSM Institute of Engineering and Technology, Dindigul, Tamil Nadu, India
[b] Department of Electronics and Communication Engineering, University College of Engineering, Anna University Tiruchirappalli, Tamil Nadu, India
[c] Department of Computer Science and Engineering, SSM Institute of Engineering and Technology, Dindigul, Tamil Nadu, India

ARTICLE INFO

ABSTRACT

Ad hoc sensor networks are the very popular network and play a vital role for producing high performance. In existing networks techniques has not perfectly balanced both energy and security in ad hoc sensor networks and gathering sensed information in an energy efficient manner is critical to operating the sensor network for a long period of time. In this research, we concentrate about security and network traffic issues. To over come this issues we have proposed a novel technique focused on Security based Data Aware Routing Protocol (SDARP) for high data gathering, to attain balancing between security and energy metrices. The security model contains two phases in first phase is here Optimal Cluster Head (OCH) is used to monitor the behavior of CH and cluster members. In second phase, security based energy efficient model is enhanced with data gathering algorithm to encrypt and decrypt with energy metrics. The proposed protocol is simulated using network simulation tool.

1. Introduction

Wireless sensors are small devices with limited energy without energy backup; they are more of one-time-use sensors [1]. A wireless ad hoc network are majorly divided into types of wireless network suc as (WANET) [2] wireless ad hoc network or Mobile ad hoc network (MANET) [3] is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks Security and energy become major issues, it should be concentrated throughout the communication in WSN. Sensor networks have the self-organizing feature and thus the automatic selection of sender and receiver is applicable hence security become a milestone in WSN [4].

Therefore, an energy-efficient routing mechanism would mean longer sensor lifetime and higher network efficiency. Active research is going on in the field of routing in ad hoc sensor networks [5]. In there are lot of development in ad hoc such as security aware routing, energy routing techniques. Secure and Energy Aware Routing Protocol. This two factors are most important contribution of the AODV. Energy-aware routing protocol (EARP) suitable for ad hoc wireless sensor networks and presents an analysis for its energy consumption in various phases of route discovery and maintenance [6, 7]. Based on the energy consumption associated with route request processing, EARP advocates the minimization of route requests by allocating dynamic route expiry times. In contrast to AODV, EARP reduces the repeated flooding of route requests by maintaining valid routes for longer durations [8].

In Some previous existing algorithms proposed scheme base on clustering to address concerns such as security and energy based routing methods in sensor networks. When the ad hoc networks is absence while the nodes can be easily compromised by attackers [9]. The internal attackers try to eavesdropping between source and sink node [10]. The external attackers try to damage the network performance. Security is a major concern which will provide authentication to the network. In this work, both authentication and network lifetime is improved by providing encryption and decryption scheme. Background work concerning the topic is discussed in the section 2. Section 3 deals with the Performance of SDARP development model. Section 4 presents about the various phases involved with simulation model. The paper concluded in Section 5. Conclusion of this paper presented in section 5.

2. Previous work

Jing Xu et al. [11] has proposed the maximum likelihood based estimation method to find the position of sensor nodes during mobility scenarios. All nodes were moving randomly to communicate with each