Secure Buffer-Based Routing Protocol for WMN

Geetanjali Rathee, Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, India
Hemraj Saini, Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, India

ABSTRACT

Secure routing is considered as one of a key challenge in mesh networks because of its dynamic and broadcasting nature. The broadcasting nature of mesh environment invites number of security vulnerabilities to come and affect the network metrics drastically. Further, any node/link failure of a routed path may reduce the performance of the entire network. A number of secure routing protocols have been proposed by different researchers but enhancement of a single network parameter (i.e. security) may affect another performance metrics significantly i.e. throughput, end to end delay, packet delivery ratio etc. In order to ensure secure routing with improved network metrics, a Secure Buffer based Routing Protocol i.e. SBRP is proposed which ensures better network performance with increased level of security. SBRP protocol uses buffers at alternate positions to fasten re-routing mechanism during node/link failure and ensures the security using AES encryption. Further the protocol is analyzed against mAODV protocol in both static and dynamic environment in terms of security, packet delivery ratio, end to end delay and network throughput.

KEYWORDS

Advanced Encryption Standard, Buffered Routing, Fault Tolerance, mAODV, Secure Routing Protocol

INTRODUCTION

The dynamic nature of mesh network makes it as a new key generation technology (Khan & Pathan, 2013). To provide a broadband connectivity with better services, several technologies have been evolved from which WMN has paid a significant role in wireless networking field (Bicket et al., 2007).

Mesh network (as depicted in Figure 1) consists of static routers called Mesh Routers which are generally used to forward the data packets among source and destination and Mesh Clients which are dynamic and accesses the network services from the internet. Routing in mesh network is one of a key challenge because of its broadband and dynamic nature. Further to route the data packet, security is one of a key concern in today’s network. Several routing algorithms have been proposed by altered researchers but as the parameters are considered, the increment of a single parametric value may reduce the other parameters drastically (Rathee & Saini, 2013; Wang et al., 2016; Meng et al., 2013). The objective of this manuscript is to design a routing protocol which route the data packets with security to the destination node and enhance more than one parametric value i.e. throughput, security attack, packet delivery ratio and end to end delay. Several routing algorithms have been proposed by different researchers (Boushaba et al., 2016; Neumann et al., 2016; Jhaveri et al., 2016). Reactive and proactive are the two routing protocol which are generally used to route the data packets.
The depicted Table 1 discussed some of the current routing protocols proposed by different researchers with their limitations. AODV-CGA, LHAP, LAAA are the protocols which secures the data packets using some technique such as 4-way handshake, digital signatures etc. but leads to some privacy and computational overhead concerns (Lu et al., 2009). Further, mAODV protocol is designed which re-route the data packets during faulty nodes. In our work, we have proposed a secure fault tolerant routing protocol which is resilient against node/link failure. In this, the basic mechanism of mesh nodes is used where each node acts as a router and has the capability to retransmit the data packets. In (Asherson & Hurchison, 2006), a secure routing protocol is designed where instead of rebroadcasting the error packets to source node during node/link failure, mesh node itself reconstruct the path and forward the data packets to destination node. The approach may reach to certain results but limited to data packet loss ratio, security and privacy concerns.

**MANUSCRIPT CONTRIBUTION**

This manuscript proposed a buffered based routing protocol called Secure Buffered based Routing Protocol (SBRP) where during any node/link failure, buffered nodes reroute the data packets without any delay and loss of a single data packet. In addition to this, AES security technique is used where the data packets are transmitted in encrypted form to prevent from forging and packet modification.
Information and Function Chunks as Building Blocks in the Control Room of Life
[www.igi-global.com/chapter/information-function-chunks-building-blocks/8194?camid=4v1a](www.igi-global.com/chapter/information-function-chunks-building-blocks/8194?camid=4v1a)

Telecommunication Management Protocols
[www.igi-global.com/chapter/telecommunication-management-protocols/21685?camid=4v1a](www.igi-global.com/chapter/telecommunication-management-protocols/21685?camid=4v1a)