Secure Modified Ad Hoc On-Demand Distance Vector (MAODV) Routing Protocol

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

ABSTRACT

In the context of wireless technology, a secure communication is requisite for stopping the unauthorized access to the network services. This manuscript's aim is to detect and eliminate the malicious nodes involved during routing path formation in mesh environments by doing some amendments in basic AODV routing phenomenon. The proposed mechanism is further merged with previously proposed secure authentication and signature routing (SASR) protocol to address the security threats such as grey hole, black hole attacks and to recover the network metrics in terms of packet loss ratio, packet delivery ratio, computational time and network throughput. Further, the approach is simulated by computing the network throughput in both the scenarios i.e. with the involvement of malicious nodes and without involvement of malicious nodes. Moreover, we have validated the network metrics of proposed mechanism against conventional approaches.

KEYWORDS
Routing Attacks, Secure AODV, Secure Routing, Threshold Signature Technique, Wireless Mesh Network

INTRODUCTION

As Wireless Mesh Network (WMN) (Khan & Pathan, 2013; Rathee & Saini, 2016) has gradually becoming a prevailing replacement technology with reasonable cost effective emulsion for last mile connectivity to the community and family networking, it is domineering to enterprise a safe and proficient communication protocol. In WMN, security can be easily conceded due to its distributed, broadcasting and dynamic nature. Therefore, an ornate authentication mechanism (Lai et al., 2016; Rathee & Saini, 2016; Martins et al., 2016; Rathee & Saini, 2016) and a secure routing (Rathee & Saini, 2015; Babbitt et al., 2016; Boushaha et al., 2016; Rathee & Saini et al., 2016) protocol should be indispensable to assure that only trusted nodes have access to various amenities with efficient network performance. Various researchers/scientists have proposed several secure routing mechanisms by introducing numerous cryptographic and trust based schemes. SAODV (Lu et al., 2009) is a protected form of AODV protocol which uses digital signatures and hash chains to implement the security inside the network. In this scheme, hash chains are used to protect the hop counts in the routing packet field while digital signature secures the routing messages. The originating node recruits the route-finding process by engendering Time-To-Live (TTL) value and seed the number with determined
hop count. Although SAODV is robust against alteration of sequence number attacks, hop count and prevents the hop count filed in routing messages from reducing, however, it does not offer hop by hop authentication and attacker may still increase the hop count to distress the routing decision of the node. Moreover, SAODV fortifies the routing messages but does not assure the integrity and authentication of the packets coming from a node. Further, the author have proposed an AODV-CGA (Asherson & Hutchison, 2006) protocol which is an addition of AODV routing mechanism designed to forward the data packets to the adjoining one in the incidence of numerous access points in WMN. The basic idea of AODV-CGA is connection of altered access points under a conjoint gateway. The author claims that the AODV-CGA is translucent to the nodes. The authors have suggested an SEAODV (Li et al., 2010) routing protocol which is based on Pre-Distribution Keys (PDK) to compute the secret pairwise transient key PTK i.e. RREP (Route Reply) for authenticating the unicast messages and Group Transient Key (GTK) to validate the broadcast messages i.e. RREQ (Route Request). The limitation of this protocol is that it is vulnerable against computation and communication overhead. RAOLSR (Saavedra et al., 2014), another secure routing mechanism implemented a combination of elliptic curve digital signature and identity based encryption algorithms to secure the messages in link state routing and last but not least (Sbeiti et al., 2014) have proposed a combination of digital signature with light weight authentication tree and symmetric block ciphers to secure the routing messages. Although researchers have proposed several cryptographic routing schemes, however, none of these protocols cannot be well adopted in WMN environment because of their high computational and communication overhead. Later researchers have proposed various trust based routing mechanisms to overcome the mentioned limitations i.e. the authors have proposed a mesh routing algorithm known as HOVER (Mir et al., 2008) which is based upon basic AODV routing protocol. The researcher gave a routing algorithm having optimal link selection and quality estimation capabilities.

Further, (Neumann et al., 2016) have suggested a decentralized secure routing mechanism by establishing the trust among individual and concurrent routing topologies. The proposed protocol protects the routed message against control plane and data plane attacks. Moreover, (Talawar & Ramesh, 2015) have proposed a secure end-to-end communication using trust node mechanism established through a shared secret key between the neighbors. Now, the basic assumption of all these routing protocols is that all the gateways and routers are cooperative and non-malicious. Some scientists/researchers have proposed secure routing protocols but these are intended for ad-hoc networks and cannot adopt well in heterogeneous environment. The existing secure routing protocols cannot adopt well in heterogeneous environment of WMN due to its dynamic and broadcasting nature and causes passive eavesdropping and decrease in network metrics i.e. packet loss ratio and end to end delay because of their low computational ad communication overheads. Further these protocols are vulnerable to a variety of security threats i.e. black hole and grey hole attacks (Patel & Jhaveri, 2015; Rathee & Saini, 2016). So, one of the severe hitches in IEEE 802.11 WMN is the design of apt secure routing protocol which can grip unpredictable vigorous topological variations and multi-hop transmission of broadband facilities. Smooth provision of broadband facilities over a multi-hop mainstay is a stimulating task and is one of the foremost reasons of recital degradation (Jia et al., 2015; Darehshoorzadeh et al., 2015; Salima et al., 2015) i.e. poor Packet Delivery Ratio (PDR) and security attacks in WMN. However, to prevent from these loopholes, a secure routing is still needed.

A previous work has been carried out for secure authentication and signature routing protocol (SASR) (Rathee & Saini et al., 2016) for reducing computational overhead and response time. The proposed protocol certifies the authenticity of mesh nodes efficiently and overlays the way for secure communication using Diffie Hellman key exchange protocol which reduces the bandwidth allocation for the key. Due to dynamic nature of WMN and involvement of number of intermediate mesh routers during communication between source and destination, there is chance of involvement of security threats from passive traffic analysis to DOS, black hole, grey hole attacks and makes the design of WMN a challenging issue.
Learning From Imbalanced Data
www.igi-global.com/chapter/learning-from-imbalanced-data/214631?camid=4v1a

Regulatory Framework of Mobile Commerce
www.igi-global.com/chapter/regulatory-framework-of-mobile-commerce/183285?camid=4v1a