International Journal of Information Security and Privacy
Volume 12 • Issue 1 • January-March 2018

Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN

Geetanjali Rathee, Jaypee University of Information Technology, Solan, India
Hemraj Saini, Jaypee University of Information Technology, Solan, India

ABSTRACT

Recently, Wireless Mesh Network is deliberated as a significant technology due to its self-healing and self-organizing characteristics. In WMN, data is forwarded through multiple hops to the destination node. One of the factors that impact the network performance is the secure communication delay. An authentication technique having significant delay may enhance the possibility of several security threats. A number of authentication protocols have been proposed in the literature but if existing practices are deliberated then to optimize one of the constraint other parameters are affected radically. In this manuscript, a Diffie-Hellman elliptic curve technique is used over WMN which reduces latency and computational overhead issues. Further to prove the integrity of proposed work, the performance is measured theoretically and analyzed experimentally over ns2 simulator.

KEYWORDS

Authentication, Cryptography, Delay, Domain, Elliptic Curve, Overhead, Security, WMN

INTRODUCTION

WMNs are the most admired proxy technology for last mile anchor for home, community and proximate networks (Akyildiz & Wang, 2005). In WMNs, security (Fu, He, Wang et al., 2008) can be easily compromised due to distributed, broadcasting and dynamic nature. Thus, an elaborate authentication mechanism is required to guarantee only trusted nodes to have access to the services. Many researchers have proposed several authentication mechanisms based on symmetric or public key cryptosystem (A. S. Wander, Gura, Eberle et al., 2005) but none of them have focused on authentication delay.

With the ease of authentication protocol, delay is taken to be an important parameter. A large delay authentication mechanism leads to a variety of threats i.e. network layer attacks, passive eavesdropping, throughput delay and so on. Authentication delay is defined as how much time is required to prove the authenticity of two nodes. Let us consider a scenario where node 'A' wants to send some information to node 'B' using an authentication protocol as depicted in Figure 1. Suppose the time taken for authentication verification of node 'A' is 4 seconds as the distance between node 'A' and node 'B' is 4 hops.

In this, if an attacker attacks between the paths, it may leads to a variety of threats. In this manuscript, several authentication schemes are discussed which are focused on delay and gives an appropriate solution over it.

DOI: 10.4018/IJISP.2018010104

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

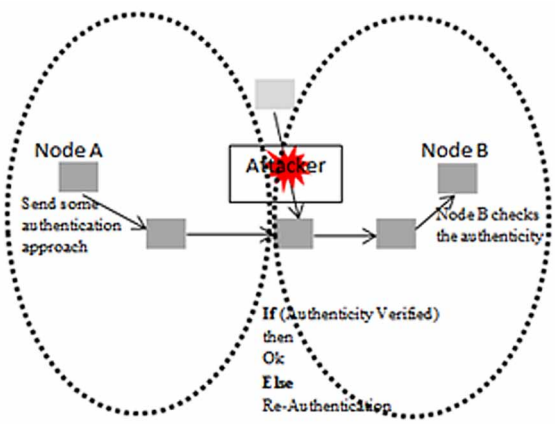
RELATED WORK

The transmit nature of communication depends on the median nodes for multi-hop conduction which occurs various security vulnerabilities in wireless mesh networks. In WMN, authentication is endorsed in two transmitting groups (either a set of MCs or MR) to recognize the legitimacy.

Symmetric and public key cryptosystems are the two ways to provide authentication in WMN. GSM networks used symmetric cryptosystem and provide mutual authentication between VLR (Visited Location Register) and mobile devices (Tang & Wu, 2008). However, the scheme may suffer from DOS attack at HLR and cause long latency in multi hop WMN. Public key cryptosystem is used by EAP standard provide an authentication infrastructure between servers and clients. The methods of Public key cryptosystem are quite complex and lacks the ability to meet the requirement for MC's. In order to reduce authentication delay in WMN, a number of schemes have been proposed in the literature. In (Aziz and Diffie, 1994) Aboba pointed out that 50ms in video conferencing and 150ms in streaming media must be ensured to provide a quality user experience. But every EAP based 802.1x limits the authentication delay min of 1000ms and 250ms during fast resume mode. Akbar and khan (Daly, Zarai & Kamoun et al., 2011) proposed a multi-hop authentication scheme which is based on EAP-TTLS (Tunneled Transport layer security). In this the minimum authentication delay is achieved up to 250ms. Further Lee et. Al. (I. Lee et al., 2007) proposed a distributed authentication method in which several trusted nodes are distributed among multiple domains of WMN. ID based cryptography is proposed by Zhang et. Al. (Y. Zhang et al., 2007) give a novel user broker operator trust model. All these approaches are available for single hop authentication. He, Joshi, Agrawal et al. (He, Joshi, Agrawal et al., 2010) proposed a de-centralized generation mechanism and provide multi-hop authenticity using symmetric polynomial based key generation. Although the authors are able to reduce in average authentication delay up to 100ms but suffers from other drawbacks i.e. DoS attack, computational overhead, passive eavesdrop etc. Authentication delay in multi hop scenario is quite difficult because messages have to travel multiple hops between source and destination. Thus, the requirement of QoS and security services, a fast and reliable authentication schemes need to be designed.

In this paper, ECDH (Lederer, Mader, Koschuch et al., 2009) mechanism is analyzed over WMN which provide the authentication between source and destination without involvement of intermediate nodes and reduce authentication delay at maximum level.

Figure 1. Message transmission



9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/authentication-through-elliptic-curve-cryptography-ecc-technique-in-wmn/190855

Related Content

Cyber Security Policy in India: Examining the Issues, Challenges, and Framework
Kush Kalraand Bhanu Tanwar (2023). *Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 120-137).*
www.irma-international.org/chapter/cyber-security-policy-in-india/313863

Energy and SLA Efficient Virtual Machine Placement in Cloud Environment Using Non-Dominated Sorting Genetic Algorithm
Oshin Sharmaand Hemraj Saini (2019). *International Journal of Information Security and Privacy (pp. 1-16).*
www.irma-international.org/article/energy-and-sla-efficient-virtual-machine-placement-in-cloud-environment-using-non-dominated-sorting-genetic-algorithm/218842

A TAM Analysis of an Alternative High-Security User Authentication Procedure
Merrill Warkentin (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 2114-2129).*
www.irma-international.org/chapter/tam-analysis-alternative-high-security/23212

E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems
Harold Pardue, Jeffrey P. Landryand Alec Yasinsac (2011). *International Journal of Information Security and Privacy (pp. 19-35).*
www.irma-international.org/article/voting-risk-assessment/58980

Analyzing Online Customer Satisfaction: The Impacts of Perceived Benefits, Perceived Risks, and Trust
Jennifer H. Gao (2019). *International Journal of Risk and Contingency Management (pp. 1-12).*
www.irma-international.org/article/analyzing-online-customer-satisfaction/216866