

ABSTRACT

Over the past 20 years, wireless technology has grown massive, and especially in the past decade wireless technology has completed a big jump almost all devices on local networks are trying to connect wirelessly. This technology is standardized by IEEE 802.11 group which is the standard for wireless local area networks.

In this paper, we propose analytical approaches based on formulas that are evaluated as system reliability using Reliability Block Diagram. System reliability is closely related to the availability of distribution or service.

Security holes in wireless technology were found in the management framework process, specifically when devices were first interconnected. We tested them to try reliability with several attack simulations using modules ESP8266 which we practice for nine access point devices at certain locations.

Our evaluation showed that the proposed solution successfully identifies and the system survives the attack with uninterrupted communication obvious on the wireless network. The results gave more than 90% reliability, were validated by using Reliability Analytics Toolkit

Keywords: ESP8266, k-out-of-n system, reliability block diagram, reliability of computer system, wireless IEEE802.11

UNIVERSITAS
MERCU BUANA

ABSTRAK

Selama 20 tahun terakhir teknologi nirkabel telah berkembang dengan sangat “massif” dan terutama dalam dekade terakhir teknologi nirkabel ini telah membuat lompatan besar karena hampir semua perangkat di jaringan lokal dihubungkan secara nirkabel, teknologi yang distandardkan oleh IEEE menjadi kedalam kelompok 802.11 yang merupakan standar untuk jaringan lokal atau WLAN yang mengatur fungsional dan kinerja.

Dalam makalah ini menjelaskan konsep dan mengusulkan pendekatan analitis berdasarkan formula yang dievaluasi sebagai keandalan sistem menggunakan Reliability Block Diagram (RBD), keandalan sistem berkaitan erat dengan ketersediaan distribusi atau layanan.

Dalam penelitian sebelumnya “lubang” keamanan dalam teknologi nirkabel ditemukan dalam proses *management frame*, yaitu ketika perangkat pertama kali saling terhubung, kemudian pengujian dilakukan untuk mencoba keandalannya dengan beberapa simulasi serangan menggunakan modul ESP8266 yang diprogram sebagai penyerang yang digunakan pada sembilan perangkat accesspoint pada suatu lokasi tertentu.

Penelitian ini mengevaluasi dan menunjukkan bahwa solusi yang diusulkan berhasil mengidentifikasi dan sistem selamat dari serangan dengan komunikasi tanpa gangguan pada jaringan nirkabel, dengan perhitungan yang menghasilkan lebih dari 90% reliabilitas, kemudian divalidasi dengan menggunakan aplikasi reliability analytics tools.

Kata kunci: *ESP8266, k-out-of-n system, reliability block diagram, reliabilitas sistem komputer, Standar IEEE802.11*