

**Ensure Data Integrity of Routing Protocols in
Underwater Wireless Sensor Networks Using SHA256 and Impact on
Power Consumption**

Prepared by:

Rahaf M. Al-Mistarihi

Supervisors:

Dr. Belal Abu Haija

Co-Supervisor:

Dr. Ahmad Al-Khasawneh

ABSTRACT

Recently, the domain of Underwater Wireless Sensor Networks (UWSNs) had received a lot of attention due to its significant advanced capabilities in ocean surveillance, marine monitoring, and application deployment for detecting underwater targets. Due to the nature of UWSNs, many security concerns arise in this area of research. Hence, the motivation for this thesis proposal is to secure routing protocol data using hash algorithm and encryption algorithm to study and measure the impact of security on power-consumption in UWSNs.

The proposed method is based on Network Simulator 2 (NS2) with routing protocols, namely, Vector Dependent Forwarding (VBF) and Hop-by-Hop Vector based Forwarding (HH-VBF) protocols, using hashing with SHA-256 and SEA Symmetric encryption to simulate the additional power consumption if any in UWSNs during routing protocols data forwarding. The three scenarios under study are as follows: first, with no security addition to the routing protocols, second, using SHA-256, and third, using symmetric encryption. The simulation findings show that power consumption in HH-VBF with the three scenarios, yields the similar results and no effect on the power-consumption. However, the VBF power consumption show noticeable change when using hashing or encryption for various data runs, the VBF best finding was with using SHA-256

التأكد من سلامة بيانات بروتوكولات التوجيه في شبكات الاستشعار اللاسلكية تحت الماء باستخدام
SHA256 وأثرها على استهلاك الطاقة

اعداد:

رهنف محمد المستريحي

إشراف:

د. بلال أبو الهيجاء

مشرف مساعد:

د. أحمد الخصاونة

الملخص

حظي مجال شبكات الاستشعار اللاسلكي تحت الماء (UWSNs) بالكثير من الاهتمام نظراً
لقدرته المتقدمة والهامة في مراقبة المحيطات والمراقبة البحرية للكشف عن الأهداف تحت الماء. كما
تشكلت العديد من الاهتمامات في تأمين حماية هذه الشبكات نظراً للطبيعة التي يتم تطبيقها فيها؛ لذلك
فإنّ هذه الدراسة تسعى إلى تأمين بيانات بروتوكول التوجيه باستخدام خوارزميات التجزئة وخوارزميات
التشفير لدراسة وقياس تأثير الأمن على استهلاك الطاقة في UWSNs. وتعتمد الطريقة المقترحة على
محاكاة NS2 مع بروتوكولات التوجيه مثل بروتوكولات VBF و HH-VBF باستخدام التجزئة مع

SHA-256 والتشفير المتماثل **SEA** لمحاكاة استهلاك الطاقة الإضافي إن وجد في أثناء إعادة توجيه

بيانات بروتوكولات التوجيه.

السيناريوهات الثلاثة قيد الدراسة هي (1) بدون إضافة أمنية إلى بروتوكولات التوجيه، (2) باستخدام **SHA-256**، (3) باستخدام التشفير المتماثل. وتظهر نتائج المحاكاة استهلاك الطاقة في **HH-VBF** مع السيناريوهات الثلاثة، وتؤدي إلى نتائج مماثلة وليس لها تأثير على استهلاك الطاقة. ومع ذلك، يُظهر استهلاك طاقة **VBF** تغييرًا ملحوظًا عند استخدام التجزئة أو التشفير لعمليات تشغيل البيانات المختلفة، وكان أفضل اكتشاف لـ **VBF** هو استخدام **SHA-256**.