البحث الأول

أولا: الملخص باللغة العربية

من خلال هذا البحث تم دراسة العديد من أنظمة بروتوكول تأمين المفتاح المتبادل الموثق فى شبكات الاستشعارات اللاسلكية و أهم هذه الانظمة البروتوكول المقدم من أيون جان و آخرون. و قد تم عمل تحليل السرية لهذا النظام و ُأثبت أنه لا يدعم خاصية السرية المتقدمة التامة (Perfect Forward Secrecy) و هى عدم السماح للمهاجم من كسر مفاتيح التشفير لباقى العقد فى الشبكة إذا ما تم إختراق أحد العقد و كسر مفتاح الشفرة الخاص به.

و قد تم تقديم بروتوكول جديد لتأمين المفتاح المتبادل الموثق فى شبكات الإستشعارات اللاسلكية بحيث يدعم خاصية السرية المتقدمة التامة و كذلك تم إثبات أن النظام المقترح أمن من عدة هجمات أهمها:

١. إعادة الهجوم Reply Attack
٢. هجوم عدم التزامن De-synchronization Attack
٣. هجوم الخداع Impersonation Attack
٤. هجوم الوسيط Man-in-the-Middle Attack