جامعة الفيوم
كلية الهندسة
قسم الهندسة الكهربية

البحث السابع

أولا: الملخص باللغة العربية

هذا البحث يتطرق الى دراسة كيفية تأمين إدارة مفتاح التشفير لشبكات الإستشعارات اللاسلكية ، فإذا كانت هذه الشبكات تعمل فى بيئة غير آمنه فلابد الأخذ فى الاعتبار القيود الواجب مراعتها فى شبكات الإستشعارات اللاسلكية ؛ فعلى سبيل المثال الاستخدام المحدود للذاكرة ، مدى الاتصال بين عقدة و أخرى قصير و كذلك الإستخدام المحدود للطاقة.

من خلال هذا البحث ، تم دراسة العديد من أنظمة إدارة مفتاح التشفير و أهم هذه الأنظمة النظام المطروح من قبل زونج و اخرين.

تم تحليل السرية لهذا النظام و تبين أنه يعانى من مشاكل عديدة أهمها:

١. مشكلة تأمين المفتاح الخاص لكل عقدة على حدا ، فإذا ما تم إختراق المفتاح الخاص فإنه يسهل على المهاجم إختراق مفتاح الجلسة Session Key بين كل عقدة و أخرى و من ثم إختراق البيانات بينهم.
٢. ضعف السرية بصفة عامة و ذلك بسبب عدم دعم هذا النظام لبروتوكول السرية المتقدمة التامة (Perfect Forward Secrecy) و الذى بدوره يضمن تأمين تبادل البيانات بين كل عقدة و مجاورتها.
٣. يستهلك كمية كبيرة من الطاقة و الذاكرة.

لذا تم فى هذا البحث إقتراح نظام إدارة جديد لمفتاح التشفير لشبكات الإستشعارات اللاسلكية معتمدا على المشاركة السرية لمفتاح الجلسة بين كل عقدة و أخرى.

تم تحليل السرية لهذا النظام الجديد و تبين انه يتمتع بالزايا الاتية:

١. يشترط وجود آليه لتبادل إثبات الثقة بين كل عقدة و أخرى لضمان تأمين البيانات بينهما
٢. يعتبر بمثابة حائط نارى للحماية من هجمات عديدة أهمها: "هجوم الإستيلاء Captured Attack" و الذى من خلاله يحاول المهاجم الاستيلاء على أحد العقد الموجودة فى الشبكة و كسر مفتاح السرية الخاص بها و بالتالى ينجح فى إختراق الشبكة.
٣. هذا النظام قابل للتطبيق على نطاق واسع مهما كان حجم الشبكة اذا ما تم التوسع فى شبكات الإستشعارات اللاسلكية.
٤. من أهم خصائص النظام الجديد أنه اذا ما تم إختراق لاى عقدة و تم السيطرة و الإستيلاء على معلومات مفتاح السرية لها ، فإنه لا يمكن للمهاجم من إختراق باقى العقد أو كشف أى معلومات عن مفاتيح السرية لهم.

بالإضافة الى أنه تم عمل مقارنة بين النظام الجديد و الأنظمة السابقى مثل LESM and SSKM و تبين أن النظام الجديد آمن ضد هجوم الإستيلاء مقارنة بالأنظمة السابقة و كذلك يستهلك طاقة و ذاكرة أقل من الأنظمة السابقة.

يعتمد

عميد الكلية

أ.د. محمد عيسى سيد أحمد

البحث السابع (تابع)

ثانيا: الملخص باللغة الإنجليزية

Summary

Wireless sensor networks (WSNs) have acquired a lot of interest due to huge number of applications. If WSNs are deployed in inimical ambience, the nature of sensor nodes must be considered such as the limitation of memory resources, low computation ability, short communication range and energy constraints. So that it is necessary to use an efficient and secure key management scheme to avoid the mentioned limitation issues as well as to reduce the security risk.

In this paper, we propose an Efficient Secure Key Management scheme (ESKM) based on secret sharing scheme which address the above problems. The proposed scheme generates three security keys; master, cluster, and sensor keys to provide secure data communication for whole nodes in the hierarchical structure of WSNs. Compared to other key management schemes; ESKM scheme has strong security and resistance against captured and forward secrecy attacks. Finally, the simulation results show that, ESKM scheme has low energy consumption, less key storage and low communication overhead compared to the existing key management schemes.

يعتمد

عميد الكلية

أ.د. محمد عيسى سيد أحمد