الجمهورية العربية السورية
جامعة البعث
كلية الهندسة المعلوماتية
قسم هندسة النظم والشبكات الحاسوبية

دراسة و تقييم وثوقية شبكات الحاسب اللاسلكية ذات البنية التحتية

دراسة أعدت لنيل درجة الماجستير في هندسة النظم والشبكات الحاسوبية

إعداد:

المهندس نصر غسان عبد الحميد

إشراف:

الدكتور المهندس أحمد أحمد

مدرس في قسم هندسة النظم والشبكات الحاسوبية– جامعة البعث

١٤٣٨ هـ – ٢٠١٧ م

الملخص

تعتبر شبكات المركبات النقالة VANET مجموعة من السيارات المتحركة ونقط الوصول على أطراف الطريق. حيث كل سيارة تملك قدرات شبكية للاتصال مع السيارات الأخرى ومع نقط الوصول التي تؤمن لها العديد من الخدمات. لقد تم في بداية هذا البحث استخدام المحاكي NCTUns 6.0 لمحاكاة عمل هذا النوع من الشبكات وذلك نظراً لصعوبة تنفيذ السيناريو في العالم الحقيقي. حيث تم استخدام بروتوكولين توجيه (شعاع المسافة الموائم ADV ، شعاع المسافة عند الطلب النقال AODV) على مجموعة من السيناريوهات التي تحاكي إلى حد ما الواقع. وتم دراسة أداء ووثوقية الشبكة بناءاً على عدد من المعايير، لنجد أن بروتوكول شعاع المسافة الموائم ADV يتلاءم مع الشبكة كلما زادت بنيتها و آلية حركة العقد تعقيداً، حيث يقوم بتعديل حمل التوجيه من خلال تنوع حجم وتردد تحديثات التوجيه استجابةً لتدفق البيانات وحركية العقد.

من ضمن العمل على شبكات الحاسب اللاسلكية قمنا بدراسة شبكات الحساسات اللاسلكية WSN التي تتضمن مجموعة من المستشعرات (الحساسات) تقوم بالتقاط وجمع المعلومات من البيئة المراقبة ومن ثم إرسالها لاسلكيا من جهاز إلى آخر بالتعاون فيما بينها إلى محطة مراقبة.حيث تم في هذه البحث محاكاة عمل شبكة حساسات لاسلكية باستخدام المحاكي Mannasim بمعاملات مختلفة وذلك لدراسة وتقييم أداء ووثوقية كل من بروتوكول توجيه شعاع المسافة عند الطلب النقال AODV و بروتوكول توجيه الخوارزمية المرتبة المؤقتة TORA و بروتوكول توجيه الطاقة المنخفضة الموائم العنقودي الهرمي LEACH بناءاً على مجموعة من المعاملات من تأخير توصيل الرزم من طرف إلى طرف ومعدل حمل التوجيه وكمية الطاقة المتبقية في الحساسات. لنلاحظ قدرة بروتوكول LEACH على الاقتصاد في استهلاك طاقة الحساسات من خلال تقسيمها إلى عناقيد واختيار رأس لكل عنقود يقوم بالتواصل مع محطة المراقبة على خلاف البروتوكولين الآخرين حيث يتم فيهما إشراك كامل الحساسات في التخاطب مع محطة المراقبة.

وتم العمل على تقنية الوصول المتعدد بتقسيم الشيفرة CDMA كملحق لهذا الإنتاج العلمي. حيث أن اعتماد الناس على الشبكات اللاسلكية لنقل بياناتهم الهامة قد زاد بشكل واضح في الفترة الأخيرة . لذلك أصبح الحفاظ على سرية وسلامة هذه البيانات أمراً ضرورياً، وعليه فإن تقنية الوصول المتعدد بتقسيم الشيفرة CDMA التي تم إعلانها كتقنية أساسية للجيل الثالث من شبكات الاتصال اللاسلكية تقدم سرية مقبولة نوعاً ما في الاتصالات الصوتية. لكن هذه السرية تبقى بعيدة عن اعتبارها مقبولة في نقل البيانات. لذلك تم في هذا البحث دراسة وتحليل سرية البيانات وسلامتها في أنظمة الوصول المتعدد بتقسيم الشيفرة CDMA IS-95.
ودراسة أداء الاقتراح باستخدام عمليات خوارزمية تشفير معيار التشفير المتقدمAES في عملية الخلط بدلا من توليد سلسلة الخلط باستخدام مسجل الإزاحة الخطي ذو التغذية الراجعة LFSR.

لتصبح السرية المبنية ضمنيا في الطبقة الفيزيائية اعتمادا على خوارزمية AESأقوى من السرية التي تقدمها تقنية الوصول المتعدد بتقسيم الشيفرة IS-95 CDMA .

Abstract

Vehicular ad hoc network VANET is a set of moving cars and access points on the side of the road, where each car has network capabilities to connect to each other and access points that provide them by different kinds of services. In the start of this search, we use NCTUns 6.0 to simulate this kind of networks because it is difficult to do that in the real world .In this search, two routing protocols (AODV, ADV) are studied within many scenarios to achieve their performances and reliability using many metrics. We conclude that ADV routing protocol adapts quickly when the complexity of network and mobility of nodes increase. This is achieved by varying the size and frequency of routing updates.

From the work on wireless networks, we study Wireless sensor networks that contains a set of sensors that catch and collect information from watched environment, then send this information wirelessly from device to another to arrive at main station. In this search, we simulate wireless sensor networks by Mannasim simulator with different parameters, that was for studying and evaluating performance and reliability of Ad Hoc On Demand Distance Vector(AODV), Temporally ordered routing algorithm(TORA), Low-energy adaptive clustering hierarchy (LEACH) routing protocols. These parameters are average end-to-end delay, average routing load and remaining energy in sensors. So we found that LEACH routing protocol can decrease consumption of sensor energy by dividing wireless sensor networks to clusters and then choose cluster head(CH) for each cluster, this CHs communicate with the main station. whereas, in the other routing protocols, all sensors can communicate with each other and with the main station.

Then, we work on CDMA technique as a Appendix for this search. so people are relying more and more on wireless communication for critical information transmission in the last period, so the security and reliability become a necessary issue. CDMA has been identified as a major technique for 3G wireless communications. The current IS-95 CDMA provides a near-satisfactory security

solution to voice wireless communications; However, the security features provided by IS-95 CDMA are far from adequate and being acceptable when they are used for data communications.

In this research, the reliability and security weakness of the existing CDMA are studied and analyzed.

The Study of the Encrypted key stream based on advanced encryption standard (AES) that is proposed to be used in the scrambling process, instead of using the scrambling sequence generated from the 42-bit linear feedback shift register (LFSR) as in IS-95 CDMA. Ensured by AES, physical layer built-in security of the proposed scheme is much stronger than that of the IS-95 system.