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

حماية بروتوكولات التوجيه الهجينة في الشبكات اللاسلكية الموائمة

دراسة أعدت لنيل درجة الماجستير في هندسة النظم والشبكات الحاسوبية

إعداد

المهندس: جورج مطانس عساف

إشراف

الدكتورة: زينب خلّوف

أستاذ مساعد في قسم هندسة النظم والشبكات الحاسوبية /جامعة البعث/

١٤٣٧ هـ – ٢٠١٦ م

الملخص

تُعرّف الشبكات اللاسلكية الموائمة بأنها مجموعة من العقد المتعاونة، المتحركة، والمُتصلة لا سلكياً من دون وجود مدير مركزي. تأتي أهمية هذه الشبكات حين لا يمكن الاعتماد على بنية تحتية ثابتة لبناء الشبكة بسبب كلفة هذه البنية أو عدم توافرها ولا سيما في المناطق النائية أو في حالات الكوارث الطبيعية، كما يمكن استخدامها لبناء شبكة آنياً بين مجموعة من العقد كما في التطبيقات العسكرية. تتصف هذه الشبكات بأنها ذات بنية ديناميكية، تصل عقدها وصلات مكررة وغير متناظرة، بالإضافة إلى التداخل اللاسلكي.

تُعد بروتوكولات التوجيه من أهم المكونات في عمل هذه الشبكات و يُوجد بروتوكول التوجيه مساراً بين أي عقدتين في الشبكة لا يوجد وصلة مباشرة بينهما ليتم لتُوجه رزم البيانات عبر هذا المسار. هناك نوعان أساسيان للتوجيه في الشبكات الموائمة هما التوجيه الاستباقي والتوجيه التفاعلي. في التوجيه الاستباقي يتم تبادل تحديثات دورية بين العقد مما يؤدي إلى إضافة عبء كبير على الشبكة، بينما يضيف التوجيه التفاعلي تأخيراً زمنياً لاكتشاف المسارات لأن إيجاد مسار بين عقدتين يتم عند الطلب، لذلك اقتُرحت بروتوكولات التوجيه الهجينة التي تجمع بين مزايا كل من التوجيه الاستباقي والتفاعلي. نقدّم في القسم الأول من هذا البحث دراسة نظرية وتقييم أداء لأحد أشهر برتوكولات التوجيه الهجينة في الشبكات اللاسلكية الموائمة ألا وهو بروتوكول التوجيه بالاعتماد على المناطق (ZRP) ونعرضُ في القسم الثاني أهم آليات حماية رسائل هذا البرتوكول من خلال دراسة مرجعية توضح عدداً من الحلول، ثمّ نقترح حلاً معتمداً على التعمية التي تعتمد على الهوية (Identity Based Cryptography – IBC–) لحماية البروتوكول (ZRP) من هجمات مثل تزوير المسار أو هجوم الثقب الأسود من خلال استخدام خوارزمية التوقيع الرقمي (Boneh-Lynn-Shacham–BLS–). علماً أن تحقيق أداء الحل المقترح وتقييمه قد تمّ باستخدام المحاكي الشبكي (NS–2).

الكلمات المفتاحية: الشبكات اللاسلكية الموائمة، برتوكولات التوجيه الهجينة، بروتوكول التوجيه بالاعتماد على المناطق (ZRP)، التعمية التي تعتمد على الهوية(IBC)، خوارزمية التوقيع الرقمي (BLS)، المحاكي NS–2.

ABSTRACT

Mobile Ad Hoc NETwork (MANET) is a collection of cooperating wireless mobile nodes forming a network on-demand without relying on a centralized administration. These networks (MANETs) gain more importance when relying on existing infrastructure is not possible due to its cost or unavailability such as in rural areas or in case of natural disasters. Moreover, MANETs can be used in case of military operations. These Ad hoc networks have a dynamic topology, asymmetric and redundant link between their nodes, and there is radio interference between the nodes.

Routing protocol is the most important component of MANETs, routing protocol discovers a route between two nodes in the network when there isn't a direct radio link between them. After discovering a route, the source node can send data packets to the destination node through this discovered route. Basically, there are two kinds of routing protocols in MANETs, they are proactive and reactive routing protocols. However, in proactive routing, nodes of the network exchange periodic routing updates, so the proactive routing protocols cause more overhead to the network. In reactive routing, a route is discovered on demand so this kind of routing protocols causes high latency for discovering a required route. Recently, hybrid routing has been proposed, it is a combination of proactive and reactive routing taking the best features from both worlds. In the first part of this thesis we present a theoretical study of the zone routing protocol (ZRP) which is one of the most common hybrid routing protocols, then we evaluate the performance of this protocol through multiple scenarios in NS2 simulator. The second part of this thesis includes a literature review for some previous security solutions that are proposed to protect ZRP protocol from security attacks. We propose a security solution depends on using identity based cryptography (IBC) concept to protect ZRP protocol from security attacks such as bogus route attack and black hole attack. Our proposal uses Boneh-Lynn-Shacham (BLS) digital signature and it is implemented using NS-2 Simulator.

Key Words: MANETs, hybrid routing protocols, ZRP protocol, identity based cryptography, BLS digital signature algorithm, NS-2 Simulator.