المستخلص

شبكة Adhoc الجوالة (MANET) من الشبكات المستخدمة بكثرة في مجال الإتصالات، بالرغم من وجود مشكلة تطبيق السرية في عمليات إرسال البيانات وتوجيهها للمسارات. الشبكة تتكون من مجموعة من الأجهزة أو العقد (nodes) الجوالة، وهي تستخدم الإتصال اللاسلكي في التخاطب مع بعضها بطريقة غير منتظمة (Ad hoc). في هذا النوع من الشبكات نحتاج لبروتوكول توجية يكون مختلف عن بقية الشبكات الأخرى. فهناك العديد من العقد التي يمكنها الإرسال في نفس اللحظة مما يتسبب في وجود التصادمات، بالإضافة إلى أن عملية الأرسال يتم بثها (Broadcast)، وبذلك يمكن لكل العقد المشاركة في الشبكة سماع ذلك الإرسال. حالياً يوجد بروتوكولات توجية لشبكات MANET تلبي تلك الإحتياجات. ولكن ومع عدم وجود مركزية في الشبكة أصبح من الضرورة وجود آلية لسرية إرسال البيانات. هنالك العديد من المقترحات التي قُدمت لتوفير السرية لبروتوكولات التوجية في شبكات MANET (Mobile Adhoc Network)، ولكن معظمها لم يراعي أهمية الموثوقية والتحقق من العقد، وأيضاً محدودية الطاقة لدى العقد المشاركة في شبكات MANET. لذلك تم إقتراح بروتوكول توجيه ليحل مشكلة السرية في شبكات MANET، مراعياً توفير السرية للعقد ذات الإمكانيات المحدودة، عن طريق إستخدام آلية التوقيع الإلكتروني (digital signature).

في هذا البحث تم توفير آلية سرية ضرورية وفعالة لعمليات إرسال وتوجية الحزم في شبكات MANET. وفيه تم توليد وحساب التوقيع الإلكتروني مرة واحدة (one time computational scheme)، مما يقلل العبء الإضافي على العقد.

في تصميم البروتوكول تم إستخدام خوارزمية MD5 لتوليد التوقيع الإلكتروني، مع الأخذ في الإعتبار الموارد المحدودة للعقد المشاركة في شبكات MANET؛ من حيث محدودية الطاقة المبذولة لحساب التوقيع الإلكتروني، وكذلك محدودية الذاكرة التخزينية، بالإضافة محدودية نطاق الإرسال.

يتم إضافة التوقيع الإلكتروني الخاص بالعقدة عند أول رسالة ترحيب تصدرها بعد دخولها للشبكة. حيث تقوم بقية العقد بتخزين ذلك التوقيع؛ لإستخدمه فيما بعد للتحقق من هوية تلك العقدة. ويتغير ذلك التوقيع كلما تغير موقع العقدة (تبعاً لتغيير الرقم التسلسلي للعقدة). والذي يلزم أن تعيد العقدة بث رسالة ترحيب جديدة، لتعلن لبقية العقد عن مكانها الجديد وكذلك توقيعها الجديد.