ورقة بحثية مجلة مفتوحة الوصول

نظرة عامة على انترنت الأشياء

د. بشرى معلا* ، د. مثنى القبيلي**

*(قسم هندسة الروبوت والأنظمة الذكية، جامعة المنارة

البريد الإلكتروني: boushra.maala@gmail.com)

**(قسم هندسة الاتصالات والالكترونيات، جامعة تشرين

البريد الإلكتروني: mothanna.alkubeily@gmail.com)

الملخص

مع التسارع الكبير في عالم التكنولوجيا الرقمية والاتصالات، تحولت الكرة الأرضية إلى عالم افتراضي متصل مع بعضه البعض، ظهر مصطلح جديد ألا وهو انترنت الأشياء، والذي يشير إلى نوع من الشبكات لربط أي شيء بالإنترنت استناداً إلى البروتوكولات المنصوص عليها من خلال أجهزة الاستشعار لإجراء تبادل المعلومات والاتصالات من أجل تحقيق التعرف الذكي وتحديد المواقع والتعقب والمراقبة والإدارة. في هذه الورقة ناقشنا بإيجاز ماهية إنترنت الأشياء، وتطبيقاتها وخصائصها وهيكليتها.

كلمات مفتاحية – انترنت الأشياء، الأجهزة الذكية، التطبيقات الذكية

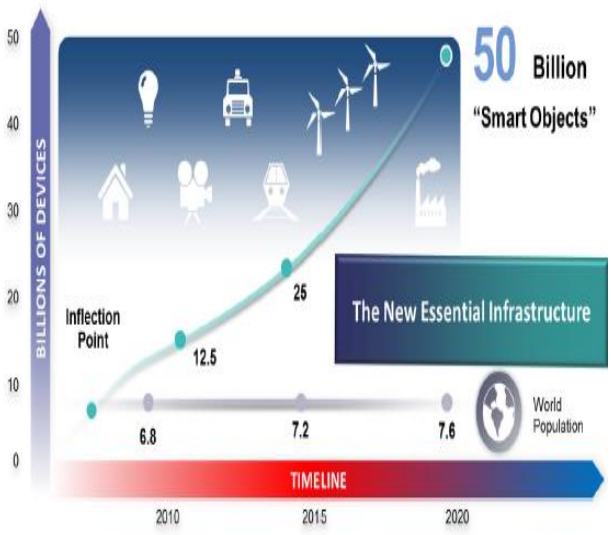
I. مقدمة

تتمثل رؤية إنترنت الأشياء في استخدام التقنيات الذكية لربط الأشياء في أي وقت وفي أي مكان ولأي شيء. ظهر إنترنت الأشياء في عام 1998، ووضع مصطلح إنترنت الأشياء لأول مرة بواسطة كيفن أشتون Kevin Ashton في عام 1999. كما يظهر في الشكل (1) تشير الدراسات إلى أنه في عام 2011 تخطى عدد الأجهزة المتصلة بالانترنت عدد سكان الأرض، و في عام 2020 أصبح العدد ما بين 26 إلى 50 بليون مستخدم [1].

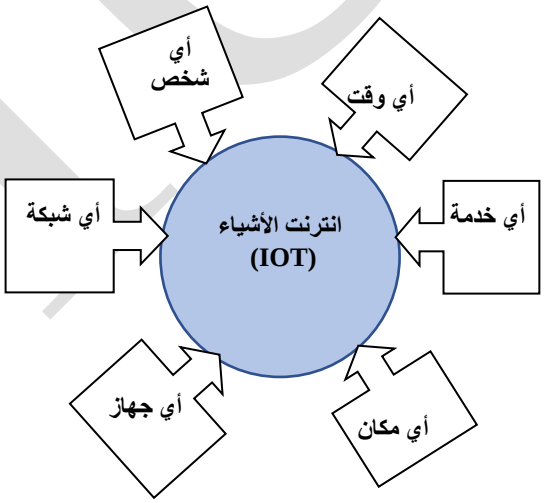
يشير إنترنت الأشياء (Internet of Things–IoT) إلى استخدام الأجهزة والأنظمة المتصلة بذكاء للاستفادة من البيانات التي جمعت بواسطة أجهزة الاستشعار والمحركات المدمجة في الآلات وغيرها. من المتوقع أن ينتشر إنترنت الأشياء بسرعة خلال السنوات القادمة، وسيطلق هذا التقارب العنان لبعد جديد للخدمات التي تعمل على تحسين نوعية حياة المستهلكين وإنتاجية المؤسسات، إنه ثورة جديدة للإنترنت[2] . يتيح اتصال الأشخاص والأشياء في أي وقت وفي أي مكان وأي شيء وأي شخص، يستخدم بشكل مثالي أي شبكة وأية خدمة، كما هو موضح في الشكل (2).

التعريف الشائع لإنترنت الأشياء هو: شبكة من الأشياء المادية. لكن الإنترنت ليس فقط شبكة من أجهزة الحاسوب فلقد تطورت إلى شبكة من الأجهزة من جميع الأنواع والأحجام؛ كالمركبات، والهواتف الذكية، والأجهزة المنزلية، والألعاب، والكاميرات، والأدوات الطبية والأنظمة الصناعية، والحيوانات، والأشخاص، والمباني [4],[3].

سنسلط في هذا المقال الضوء على مفهوم انترنت الأشياء، وينظم هذا المقال على النحو الآتي، بداية سنستعرض تطبيقات إنترنت الأشياء في مختلف مجالات الحياة المتنوعة كتطبيقات المدن الذكية والزراعة والبيئة والصحة، ومن ثم نتناول خصائص إنترنت الأشياء التي تتمتع بها، وبعدها نقدم شرحاً للطبقات التي تتكون منها إنترنت الأشياء، ونختم هذا المقال بمفهوم الأمن في انترنت الأشياء من متطلبات وتحديات وهجمات قد تتعرض لها هذه الشبكات.



الشكل 1: ثورة انترنت الأشياء



الشكل 2: انترنت الأشياء (IoT)

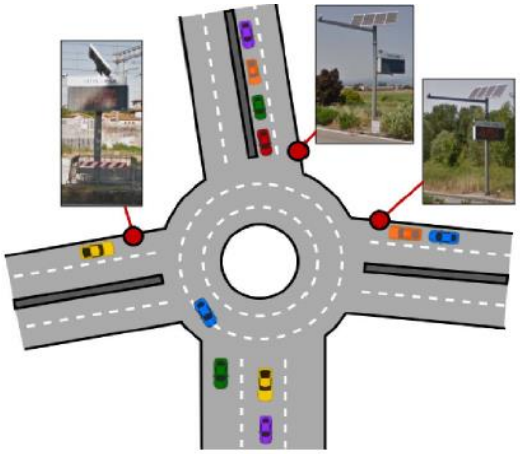
II. تطبيقات انترنت الأشياء

يوجد الكثير من التطبيقات، التي يمكن تصنيفها كتطبيقات انترنت الأشياء، نذكر فيما يأتي بعضاً منها [3] :

A. المدن الذكية (Smart Cities):

يلعب انترنت الأشياء دوراً كبيراً في جعل المدن ذكية، انظر الشكل (3)، وذلك من خلال عدة تطبيقات مثل مراقبة الحدائق في المدينة ومراقبة الاهتزازات والمكونات المادية للأبنية والجسور، ومراقبة الضجيج في الأماكن الحساسة لذلك، ومراقبة حركة العربات وربط ذلك بإشارات المرور، كما في الشكل (4)، وإضاءة الشوارع الذكية المتكيفة مع تغيرات الطقس [5].

الشكل 3: تطبيقات المدن الذكية



الشكل 4: مراقبة حركة العربات

كما يندرج تحت تطبيقات المدن الذكية الإدارة الذكية لمواقف السيارات، والتي تشكل مشكلة كبيرة في المدن الكبرى التي تعاني من الازدحام، مما يساهم في تخفيض حركة المرور في المناطق التي تكون فيها جميع مواقف السيارات مشغولة. في الشكل (5) ، يظهر مثال عن إدارة موقف السيارات الذكي حيث يتم رصد

حالة كل موقف من خلال مركز مخصص للاستشعار والمعلومات التي تم جمعها بشكل دوري، و من ثم تُستخدم البيانات التي تم جمعها لإنشاء خريطة في الوقت الفعلي لمنطقة وقوف السيارات التي يمكن توفيرها للسائقين، من خلال تطبيق معين على هواتفهم الذكية. بهذه الطريقة يتم إرشاد السائقين نحو أقرب موقف (مجاني) للسيارات، مما يوفر الوقت، ويخفض استهلاك الوقود وتلوث الهواء [6].

الشكل 5: تطبيق الموقف الذكي

B. الزراعة الذكية (Smart Agriculture):

يمكن أن تساعد إنترنت الأشياء في تحسين الزراعة من خلال مراقبة رطوبة التربة، والتحكم في الظروف المناخية الدقيقة لزيادة إنتاج الفاكهة والخضراوات وجودتها، ودراسة أحوال الطقس فيها للتنبؤ بمعلومات الجليد والجفاف والثلج أو تغيرات الرياح والتحكم في الرطوبة ومستوى درجة الحرارة لمنع الفطريات والملوثات الميكروبية الأخرى. يشمل دور إنترنت الأشياء في إدارة المياه دراسة ملاءمة مياه الأنهار والبحر للزراعة والاستخدامات الصالحة للشرب ومراقبة تغيرات منسوب المياه في الأنهار والسدود والخزانات. يبين الشكل (6) مثالاً على تطبيقات الزراعة الذكية.

الشكل 6: مثال عن تطبيقات الزراعة الذكية

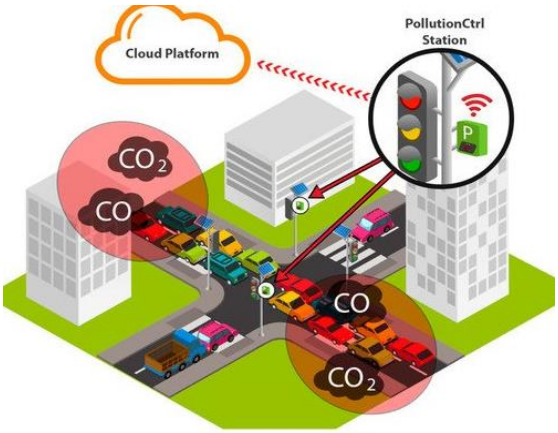
C. الرعاية الصحية الذكية (smart health):

تصنف التقنيات التي توفرها إنترنت الأشياء إلى مجال الرعاية الصحية إلى صنفين أساسيين: 1. تتبع الأشياء والموظفين والمرضى، مثلاً حالة مراقبة المرضى لتحسين سير العمل في المستشفيات 2. تحديد الأشخاص ومصادقة هوياتهم ويتضمن تحديد هوية المريض لتقليل الحوادث المؤذية للمرضى وغيرها. يظهر في الشكل (7) أمثلة على تطبيقات انترنت الأشياء في مجال الرعاية الصحية.

الشكل7: مثال على تطبيقات الرعاية الصحية

D. البيئة الذكية (Smart environment):

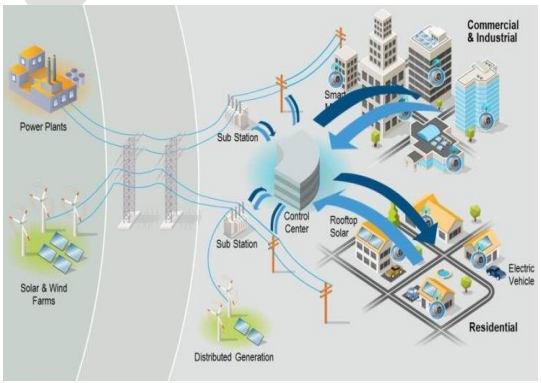
تشمل التطبيقات التي تتعلق بالطبيعة مثل مراقبة تلوث الهواء للتحكم بما تطلقه المصانع من غاز CO_2 ، أو ما ينتج عن عوادم السيارات، ومراقبة الغابات لكشف الحرائق مبكراً، ومراقبة الظروف المناخية من الرطوبة و الحرارة و الضغط. يبين الشكل 6 مثالاً يوضح إحدى تطبيقات البيئة الذكية .



الشكل8: تطبيق مراقبة تلوث الهواء الناتج عن عوادم السيارات

E. الطاقة الذكية (Smart energy):

تتضمن التطبيقات التي تجعل من مراقبة استهلاك الطاقة هدفاً لها مثل مراقبة وتحليل تدفق الطاقة من العنفات و في المنازل، التحكم بكمية الطاقة المطلوبة وتحسين فعالية الطاقة بضياعات أقل من مصادر الطاقة المتعلقة بأجهزة الحاسوب وغيرها من الأجهزة الالكترونية. تظهر في الشكل (9) إحدى هذه التطبيقات:



الشكل9: تطبيق ذكي لمراقبة وتحليل تدفق الطاقة

III. خصائص إنترنت الأشياء

تتمتع إنترنت الأشياء بالعديد من الخصائص نذكر فيما يأتي بعضاً منها[4],[3] :

1) الترابط (Interconnectivity):

تضمن انترنت الأشياء ربط أي شيء بالبنية التحتية العالمية للمعلومات والاتصالات.

2) عدم التجانس(Heterogeneity):

إن الأجهزة المكونة لإنترنت الأشياء غير متجانسة لأنها تعتمد على منصات وشبكات أجهزة مختلفة، قد تكون حساسات لاسلكية أو أجهزة خلوية أو غيرها.

3) التغييرات الديناميكية (Dynamic changes):

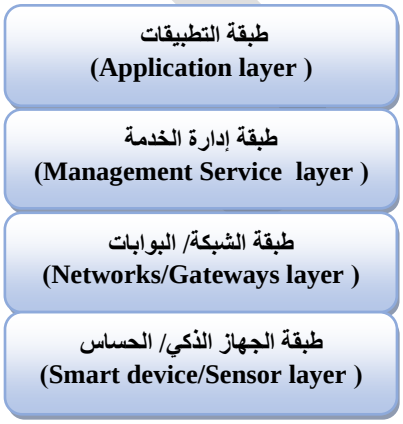
تتغير حالة الأجهزة ديناميكياً، على سبيل المثال، التغير بين حالتي النوم والاستيقاظ، والاتصال والانقطاع، وقد يكون أيضاً الموقع والسرعة بالنسبة للأجهزة المتحركة. علاوة على ذلك، يمكن أن يكون عدد الأجهزة المتصل متغير ديناميكياً.

4) الحجم الهائل (Enormous scale):

إن عدد الأجهزة التي يجب إدارتها والتي تتواصل مع بعضها سيكون أكبر من حيث الحجم من الأجهزة المتصلة بالإنترنت حالياً. هنا تظهر أهمية إدارة البيانات المتبادلة بين هذه الأجهزة ومعالجتها والاستفادة منها حسب التطبيق.

IV. بنية انترنت الأشياء (IOT ARCHITECTURE) :

تتكون من عدة طبقات داعمة لتقنية انترنت الأشياء، سنورد فيما يأتي بنية انترنت الأشياء الأكثر شيوعاً [7] والتي تتكون من 4 طبقات كما في الشكل (10) :



الشكل 10: بنية انترنت الأشياء

A. طبقة الجهاز الذكي/ الحساس:

هي الطبقة الأدنى في هيكلية انترنت الأشياء، تتكون من التجهيزات الذكية المدمجة مع الحساسات. تؤمن الحساسات التفاعل بين العالم الرقمي والعالم الفيزيائي، ممكنة بذلك من معالجة وجمع المعلومات في الزمن الحقيقي. فالحساس يمكن أن يقيس الخاصية الفيزيائية ويحولها إلى إشارة يمكن أن تفهم من قبل الأجهزة. يوجد عدة أنواع من الحساسات لأهداف وغايات مختلفة. تملك الحساسات القدرة على أخذ القياسات مثل درجة الحرارة ونوعية الهواء والرطوبة والضغط.

يمكن أن تصنف الحساسات حسب هدف وحيد مثل حساسات البيئة وحساسات الجسم وحساسات المركبات. تحتاج معظم الحساسات أن تتصل مع حساسات أخرى تعمل كبوابات (gateway)، هذا يمكن أن يكون على شكل شبكة LAN مثل الايثرنت (سلكية) أو لاسلكية مثل WIFI أو شبكة PAN مثل الـ Zigbee أو البلوتوث والـ UWB . لا تحتاج بعض الحساسات إلى عقد مجمعة بل تتصل مع المخدم أو التطبيق.

إن الحساسات التي تستخدم طاقة منخفضة ومعدل اتصال بيانات منخفض، تشكل نوعاً من الشبكات الأكثر شيوعاً وهي شبكات الحساسات اللاسلكية WSN، والتي حازت على شعبية كبيرة من خلال إمكانية تعاملها مع عدد كبير من العقد مع الاحتفاظ بعمر البطارية وتغطي مساحات كبيرة.

B. طبقة الشبكات/البوابات (Gateway/Networks Layer)

إن حجم البيانات الكبير الناتج عن المعلومات الملتقطة من قبل الحساسات، يتطلب بنية تحتية عالية الأداء قادرة على التعامل معه، سواء كان وسط النقل سلكياً أو لاسلكي. إن الشبكات الحالية مقيدة بمجموعة مختلفة جداً من البروتوكولات، و التي استخدمت لدعم شبكات آلة إلى آلة (M–2–M) وتطبيقاتها. لذا مع ظهور الحاجة لتخديم مجال عريض من خدمات انترنت الأشياء وتطبيقاتها مثل خدمات النقل عالية السرعة، ظهرت الحاجة إلى شبكات متعددة بتقنيات متنوعة وبروتوكولات وصول لتعمل مع بعضها البعض. يمكن أن تكون هذه الشبكات من النموذج الخاص أو العام أو الهجين لتدعم متطلبات الاتصالات مثل الانتظار (latency) وعرض الحزمة والأمن.

C. طبقة إدارة الخدمة (Management Service layer):

تجعل إدارة الخدمة معالجة المعلومات ممكنة من خلال نمذجة العمليات وإدارة التجهيزات والتحليل والتحكم بالأمن. إحدى الميزات المهمة لخدمة الإدارة هي محركات قواعد الأعمال والعمليات. تجمع انترنت الأشياء بين الاتصال والتفاعل بين الكائنات والأنظمة معاً لتوفير المعلومات على شكل أحداث أو بيانات مثل درجة حرارة البضائع والموقع الحالي وحركة البيانات. إن بعض هذه الأحداث مثل التقاط البيانات التحسسية الدورية تحتاج إلى ترشيح أو توجيه إلى أنظمة ما بعد المعالجة، بينما يتطلب الآخر استجابة للحالات العاجلة مثل حالات الطوارىء المتعلقة بالظروف الصحية للمريض.

بما يخص التحليل، يوجد عدة أدوات تحليل يمكن أن تستخدم لتحليل كميات معلومات إضافية مترابطة من تدفق البيانات الكبير، ويمكن أن تعالج هذه البيانات بمعدل سرعة عال.

فمثلاً استخدام تحليل الذاكرة يخفض من زمن طلب البيانات ويزيد من سرعة اتخاذ القرار، كما أن تحليل التدفق يحدث في الزمن الحقيقي، وبالنتيجة يكون اتخاذ القرار في غضون ثوان.

يمكن حماية طبقة التطبيقات الأعلى من الحاجة إلى معالجة البيانات غير الضرورية وتخفيض مخاطر الكشف عن الخصوصية لمصدر البيانات، حيث أن تقنيات الترشيح (التصفية) مثل إخفاء هوية البيانات والتكاملية ومزامنة البيانات، تستخدم لإخفاء المعلومات الأساسية المستخدمة في التطبيقات ذات الصلة. يجب أن يفرض الأمن على كامل بنية انترنت الأشياء مباشرة من طبقة الجهاز الذكي وصولاً إلى طبقة التطبيقات. يمنع أمن النظام قرصنة النظام أو السيطرة عليه من

قبل الأفراد غير المصرح لهم بذلك، وبالنتيجة التقليل من احتمالية الخطر.

D. طبقة التطبيقات (Application layer):

تشمل التطبيقات مجال البيئات الذكية في عدة قطاعات مثل: النقل، البناء، المدينة، الزراعة، نمط الحياة، التجارة، الصناعة، الطوارىء، الرعاية الصحية، التعليم، الثقافة، السياحة، البيئة، الطاقة.

V. الأمن في انترنت الأشياء:

يعرف الأمن بأنه إجرائية حماية المصدر من الضرر المادي، أو من الوصول غير المصرح به أو السرقة، من خلال الحفاظ على سرية وسلامة المعلومات وضمان المصادقة وعدم تسرب المعلومات. بما أن إنترنت الأشياء يعتمد على اتصال عدد لا يحصى من الأجهزة لتشغيلها، فإن هنالك احتمال كبير جداً للتعرض لهجوم أمني. في تكنولوجيا المعلومات، الهجوم هو محاولة تدمير أو كشف أو تغيير أو تعطيل أو سرقة أو الوصول غير المصرح به إلى أحد المصادر. هجوم إنترنت الأشياء ليس جديداً لكن الجديد هو الحجم والبساطة النسبية للهجمات في إنترنت الأشياء (IoT)، إن الملايين والمليارات من الأجهزة يمكن أن تكون ضحية محتملة للهجمات السيبرانية التقليدية [8].

فمثلاً أجري تحليل من قبل الباحثين في [9] أظهر أن 13% من 156680 جهاز متصل كان عرضة لثغرة أمنية.

VI. متطلبات الأمن في شبكات انترنت الأشياء:

يجب مراعاة تحقيق الأمن طوال دورة حياة إنترنت الأشياء، وذلك بدءاً من التصميم الأولي وحتى تشغيل الخدمات. تتضمن متطلبات الأمن الرئيسية في سيناريوهات إنترنت الأشياء المصادقة والترخيص والسرية والموثوقية، فيما يأتي نورد شرحاً لكل من هذه المتطلبات:

A. موثوقية البيانات (Data confidentiality):

يجب أن تكون البيانات التي ترسلها أو تستقبلها العقدة موثوقة ويتحقق ذلك من خلال الدمج ما بين السلامة والموثوقية عن طريق التشفير. على سبيل المثال، في شبكات الجسم اللاسلكية إرسال القيمة الممثلة لمقياس السكر يجب أن ترسل بحيث يكون من المضمون وصولها دون ان تتعرض إلى تغير مفاجيء أو أن يطلع عليها أحد غير مصرح له بذلك حفاظاً على سرية بيانات المريض، ويكون ذلك باستخدام التشفير، رغم وجود تحديات تخص تطبيق تقنيات التشفير كالذاكرة المحدودة وقدرة المعالج المحدودة أيضاً [10].

B. السرية (Privacy):

لا يزال الحفاظ على السرية في إنترنت الأشياء يمثل تحدياً كبيراً [11],[12]. تتضمن السرية أمن المعلومات الشخصية إضافة إلى القدرة على التحكم فيما يحدث لهذه المعلومات. إن مشاكل السرية مع أنظمة إنترنت الأشياء معقدة، وذلك بسبب حقيقة أن النظام أكثر من مجموعة من الأجزاء. قد تختلف اعتبارات السرية للأجهزة منخفضة المستوى عما هو عليه في مستوى التطبيق أو تحليل البيانات. لكن في الوقت نفسه، إن انتهاكات السرية على أي مستوى في النظام سيؤثر على النظام بأكمله.

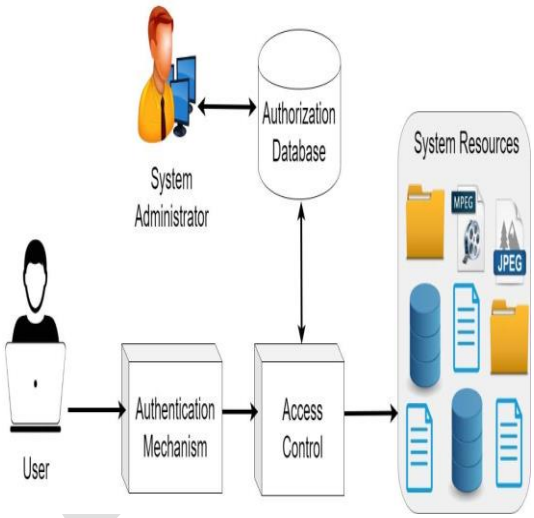
إن جمع الكثير من المعلومات الخاصة من الأجهزة الذكية، والتحكم في هذه المعلومات ضعيف في تقنيات إنترنت الأشياء الحالية. في كثير من الحالات يتم جمع البيانات بشكل يسبب حدوث انتهاكات للسرية دون أن يلاحظها أحد لفترة طويلة.

في بعض الحالات، قد لا يكون المستخدم على معرفة بأن جهاز إنترنت الأشياء يقوم بجمع بيانات حول الفرد وربما يشاركها مع أطراف ثالثة. أصبح هذا النوع من جمع البيانات أكثر شيوعًا في الأجهزة الاستهلاكية مثل أجهزة التلفزيون الذكية والمساعدين الشخصيين الأذكياء.

C. المصادقة والترخيص (authentication and authorization):

إن تقنيات المصادقة والتحكم بالوصول لها أهمية كبيرة في إنترنت الأشياء. دون وجود آلية مناسبة للتحكم بالوصول، يمكن اختراق بنية إنترنت الأشياء بالكامل، نظراً لأن أجهزة إنترنت الأشياء تعتمد بشكل كبير على مصداقية المكونات الأخرى المرتبطة بها. وبالنتيجة، فإن وجود آلية مناسبة للتحكم بالوصول أمر بالغ الأهمية لتخفيف العيوب في البنية التحتية الحالية لإنترنت الأشياء [13].

تتكون آليات التحكم في انترنت الأشياء من مرحلتين أساستين هما : 1. المصادقة 2. الترخيص، كما في الشكل (11):



الشكل 11: نظام آلية التحكم في IOT

1) المصادقة: هي عملية التحقق من هوية الكيان [14]. يمكن أن يكون الكيان المراد التحقق منه إما إنسانًا أو آلة. المصادقة هي المرحلة الأولى من أية آلية للتحكم بالوصول يمكنها تحديد الهوية الدقيقة للطرف القائم بالوصول من أجل إنشاء ثقة النظام.

في معظم الحالات، تبدأ إجرائية المصادقة بين الإنسان **والآلة لتسجيل الدخول إلى بوابة الخدمات عبر الإنترنت** وإدخال بيانات المصادقة.

الترخيص: هو عملية فرض الحدود ومنح الامتيازات للكيانات المصدق عليها [15]. بعبارات بسيطة، هذا هو تحديد قدرات كيان في النظام. لكي يسمح لكيان ما للقيام بأي إجراء، يجب التحقق من هوية هذا الكيان أولاً من خلال المصادقة. وفقًا للشكل 11، عادةً ما يقوم المسؤول بتكوين قاعدة بيانات الترخيص لمنح الوصول والحقوق إلى موارد النظام. تعين حقوق مختلفة لكل مورد مثل القراءة والكتابة والتنفيذ. اعتمادًا على مستوى التفويض (الترخيص) الذي يتم تعيينه بواسطة المسؤول، يمكن لكل كيان مصدق عليه تنفيذ إجراءات مختلفة على الموارد.

VII. المخاطر الأمنية في انترنت الأشياء:

يمكن أن نصنف المخاطر الأمنية في انترنت الأشياء إلى:

A. المخاطر النموذجية التي تحدث في أي نظام إنترنت: والمقصود بها ممارسات الأمن التقليدية مثل تأمين المنافذ المفتوحة على الأجهزة على سبيل المثال، قد تستخدم ثلاجة متصلة بالإنترنت لإرسال تنبيهات حول مخزون المنتج ودرجة الحرارة خادم SMTP غير آمن وعرضة للاختراق.

B. المخاطر الخاصة بأجهزة إنترنت الأشياء:

تشمل المشكلات المتعلقة تحديداً بأجهزة إنترنت الأشياء، على سبيل المثال قد تخترق معلومات الجهاز الآمنة، فبعض أجهزة إنترنت الأشياء صغيرة جداً بحيث لا تدعم التشفير غير المتماثل المناسب.

C. السلامة لضمان عدم حدوث ضرر:

إن سوء الاستخدام قد يسبب ضرراً في الشبكة، فمثلاً سوء استخدام المشغلات قد يتسبب بضرر لهذه المشغلات وبالنتيجة للشبكة ككل.

VIII. الهجمات على شبكات انترنت الأشياء:

قد يأتي الهجوم نفسه بأشكال عديدة، بما في ذلك هجمات الشبكة الفعالة لمراقبة حركة المرور غير المشفرة بحثاً عن معلومات حساسة؛ أو الهجمات السلبية مثل مراقبة اتصالات الشبكة غير المحمية لفك تشفير حركة المرور ضعيفة التشفير والحصول على معلومات المصادقة؛ وما إلى ذلك، فيما يأتي نذكر أنواع الهجمات الإلكترونية الشائعة هي:

A. الهجوم الفيزيائي (Physical Attack):

يعبث المهاجم في هذا الهجوم بالمكونات الصلبة. ويعود ذلك إلى الطبيعة الموزعة وغير المراقبة لانترنت الأشياء، إذ تعمل الأجهزة ضمن بيئة مفتوحة [16] .

B. هجوم الاستطلاع (Reconnaissance Attack):

هو الهجوم الذي ينتج عنه اكتشاف غير مصرح به ورسم خرائط الشبكة والخدمات أو تحديد نقاط الضعف. مثال عليه مسح منافذ الشبكة، وتحليل حركة المرور.

C. هجوم حجب الخدمة (DoS(Denial of Services Attack):

يعد من الهجومات الأكثر انتشاراً وأسهلها تنفيذاً في شبكات انترنت الأشياء، إن هدف هذا النوع من الهجوم هو محاولة جعل مصادر الشبكة غير متاحة من قبل المستخدمين، والأمر الذي يساعد المهاجم في تحقيق هدفه بسهولة هو مقدرات الذاكرة المنخفضة وقدرة المعالجة المحدودة لمعظم أجهزة شبكات إنترنت الأشياء. يمكن أن يظهر بعدة أشكال فمثلاً بالنسبة لأي شبكة لاسلكية، يعد "التشويش" على القناة بإشارة مقاطعة هجومًا فعالاً من هجومات DoS .

D. هجوم الوصول (Access Attack):

هو حصول الأشخاص غير المصرح لهم الوصول إلى الشبكة أو الأجهزة، وهم لا يملكون حق الوصول إليها. ولهذا الهجوم نوعان: النوع الأول هو وصول فيزيائي عندما يستطيع المهاجم أن يصل إلى الجهاز الفيزيائي، والوصول عن بعد ويحدث عندما يتمكن المهاجم من الوصول إلى عنوان IP لجهاز متصل.

E. التجسس السيبراني (Cyber Espionage):

استخدام تقنيات الاختراق والبرمجيات الخبيثة للتجسس أو الحصول على معلومات سرية للأفراد أو المنظمات أو الحكومات.

F. هجوم التحليل (Cryptanalysis Attacks) :

يتمثل في محاول المهاجم الذي حصل على النص المشفر تحليله بهدف الوصول إلى كسر التشفير.

G. هجوم رجل في المنتصف MITM(Man-In-The-Middle):

إن مفهوم هجوم رجل في المنتصف يتمثل بالهجوم الذي يعمل فيه المهاجم أو المتسلل على مقاطعة واختراق الاتصالات بين نظامين منفصلين. يمكن أن يكون هجوماً خطيراً لأنه هجوم يعترض فيه المهاجم سراً وينقل الرسائل بين طرفين بينما يظن فيه الطرفان أنهما يتصلان مع بعضهما مباشرة، لأن المهاجم لديه الاتصال الأصلي، لذا يمكنه خداع المستلم ليعتقد أنه لا يزال يتلقى رسالة شرعية.

يمكن أن تكون هذه الهجمات خطيرة للغاية في إنترنت الأشياء، بسبب طبيعة "الأشياء" التي تخترق. على سبيل المثال، يمكن أن تكون هذه الأجهزة أي شيء من الأدوات الصناعية أو الآلات أو العربات إلى "أشياء" غير ضارة مثل أجهزة التلفزيون الذكية أو الثلاجات الذكية أو المحركات المسؤولة عن فتح وإغلاق المرآب.

إن مصادقة الأجهزة في شبكات إنترنت الأشياء تتضمن تبادل هويات الأجهزة، لذا فإن هجوم رجل في المنتصف سيكون ممكناً من خلال سرقة الهوية [10].

IX. الخاتمة:

إن انترنت الأشياء بما تقدمه من تطبيقات ستغير وجه العالم. أنشئت العديد من فرق البحث من جميع أنحاء العالم لإجراء أبحاث متعلقة بإنترنت الأشياء. يهدف كل هذا لتمكين الاتصالات مع الكائنات الذكية وفيما بينها، مما يؤدي إلى توفير الاتصال "في أي وقت وفي أي مكان وأي وسائط وأي شيء". لذا عرضنا في هذا المقال أهم جوانب إنترنت الأشياء، والتطبيقات المختلفة لإنترنت الأشياء ومكوناتها المستخدمة. كما سلط الجزء الأخير من هذه الورقة الضوء على مسألة الأمن في انترنت الأشياء.

المراجع:

[1]. O. Vermesan, P. Friess, "Internet Of Things -from *research and innovation to market deployment",* River publisher Series communication, 2014.

[2]. V. Bhuvaneswari, and R Porkodi "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview," IEEE. Computer Science, International Conference on Intelligent Computing Applications, 2014.

[3]. K. K Patel, S. M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", May, 2016.

[4]. G. D. Amane, "An Overview of Internet of Things",13th international conference on recent innovations in science, engineering and management, February 2018.

[5]. A. Grizhnevich (2021), "IoT for Smart Cities: Use Cases and Implementation Strategies", [Online]. Available: https://www.scnsoft.com/blog/iot-for-smart-city-use-cases-approaches-outcomes

[6]. F. Righetti, C. Vallati, G. Anastasi, *"IoT Applications in Smart Cities: A Perspective Into Social and Ethical Issues",* IEEE International Conference on Smart Computing, 2018.

[7]. (2021), [Online] Available: https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf

[8]. J. Anca, R. Pasika and X. Lina. "Introduction to IoT Security". ch2 in book: IoT Security: Advances in Authentication, Publisher: John Wiley Sons Ltd. 2019

[9]. M. Abomhara and G. M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015.

[10]. M. Gloukhvtsev," IOT Security: Challenges, Solutions & Future Prospects", DELLEMC, 2018.

[11]. R. Williams, E. McMahon,S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach", 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017

[12]. X. Lu, Z. Qu, Q. Li, and P. Hui, Privacy Information security Classification for internet of things based on internet Data". International Journal of distributed sensor networks. 11(8),2015

[13]. J. Kannaiappan and B. Rajendran, "Privacy in the internet of things". In Lee (ed.). The internet of Things in the modern environment. IGI. Global. 2017.

[14]. F. Alaba, M. Othman, I. Hashem and F. Alotaibi, "Internet of Things security: A survey", Journal of Network and Computer Applications, 88, pp.10-28, 2017

[15]. M. Stamp, Information security, 2nd ed. Hoboken, N.J.: Wiley, 2011, pp. 227-278.

[16]. S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," Potentials, IEEE, vol. 21, no. 5, pp. 17–19, 2002.

منشورات المؤلف (د. مثنى القبيلي):

[1]. Alkubeily, M., Maala, B. (2021). An overview of the Internet of Things-IoT. *Al-Manara University Journal*, Vol.1, No.1.

[2]. Alkubeily, M., Hasan, B. Discover the broken paths to improve routing in UAV-assisted VANET. Tartous University Journal for Research and Science Studies, Vol.5, No.10, 2021.

[3]. Alkubeily, M., Shaweesh, R. (2021). Cheating Detection and Cancellation in (MDA-ALM) Protocol in Application-Level Multicast Networks. International Journal of Science and Research (IJSR), Vol.10, Issue.4, PP: 948-956.

[4]. Alkubeily, M., Dabaj, M. (2021). Enhancement Of Adaptive Routing Protocol In WBAN Based-On Ant Colony Algorithm. Hama University Journal, Vol.4.

[5]. Esber, Gh., Alkubeily, M., Sulaiman, S., Mehrez, A. (2020). WINDOWS FORM APPLICATION FOR VIRTUAL MINIMIZED PLATFORM KERNEL FOR WIRELESS SENSOR NETWORK SIMULATOR. Far East Journal of Electronics and Communications, Vol.23, Issue.2, PP: 61-71.

[6]. Alkubeily, M. (2020). A New Scheme to Secure Group Communication in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.42, No.5, PP: 401-417.

[7]. Alkubeily, M. (2020). Study the Effectiveness of Patient's Monitoring in Hospitals using Wireless Body Sensor Networks. Tishreen University Journal of Science and Engineering, Vol.42, No.3, PP: 25-43

[8]. Alkubeily, M., Hassan, L. (2020). Improvement Energy Consumption in Fault-tolerant Large-Scale Wireless Sensor Networks: DECROP protocol. Tishreen University Journal of Science and Engineering, Vol.42, No.3, PP: 251-270.

[9]. Alkubeily, M., Inbashi, S. (2020). Enhancing Link Reliability for GPSR-MA protocol in VANETs-Highways. Tishreen University Journal of Science and Engineering, Vol.42, No.2, PP: 201-215.

[10]. Alkubeily, M. (2019). Design an Intelligent Traffic System Based on Wireless Sensor NetworksCase Study: Lattakia City –AL ZeraaRoundabout. Tishreen University Journal of Science and Engineering, Vol.41, No.5, PP: 741-757.

[11]. Alkubeily, M., Mahmoudy, GH., Mahmoud, D. (2019). A New Study the effect of the measurement matrix on the performance of the compressed sensing of embedded images in wireless multimedia sensor networks. Tishreen University Journal of Science and Engineering, Vol.41, No.5, PP: 453-471.

Estimation in Wireless Multimedia Sensor Networks. International Journal of Science and Research (IJSR), Vol.4, Issue 11, PP: 1329-1337.

[23]. Jbeily, T., Alkubeily, M., Hatem, I. (2015). An Efficient Adaptation of Edge Feature-Based Video Processing Algorithm for Wireless Multimedia Sensor Networks. International Journal of Computer Science Trends and Technology (IJCST), Vol.3, No.3, PP: 156-166.

[24]. Alkubeily, M. (2015). Cheating Impact on Overlay Tree Construction Algorithms in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.37, No.3.

[25]. Alkubeily, M., Shawish, R. (2015). Cheating Avoidance in MDA-ALM Protocol in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.37, No.2.

[26]. Alkubeily, M., Maala, B. (2015). Fault Tolerance in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.37, No.1.

[27]. Alkubeily, M., Hatem, I., Jbeily, T. (2014). Study and Evaluation the Performance of Some DCT-Based Image Fusion Techniques in Wireless Multimedia Sensor Networks. Tishreen University Journal of Science and Engineering.

[28]. Alkubeily, M., Youness, N. (2014). Fault Tolerance Routing In Wireless Sensor Network. Tishreen University Journal of Science and Engineering, Vol.36, No.1, pp: 185-204.

[29]. Maala, B., Alkubeily, M., Raya, G. (2014). Improving Packet Delivery Ratio for On-Demand Multicast Routing Protocol (ODMRP). *Tishreen University Journal of Science and Engineering*, Vol.36, No.1, pp: 169-184.

[30]. Alkubeily, M., Bettahar, H., Bouabdallah, A. (2011). A New Application-Level Multicast Technique for Stable, Robust and Efficient Overlay Tree Construction. Computer Networks (ELSEVIER),55: 3332-3350,

[31]. Bettahar, H., Alkubeily, M., Bouabdallah, A. (2009). TKS: A Transition Key Management Scheme for Secure Application-Level Multicast. International Journal of Security and Networks (IJSN), Volume 4, number 4: 210-222.

[32]. Alkubeily, M., Bettahar, H., Bouabdallah, A. (2008). Impact of Cheating and Non-Cooperation on the Stability and the Performances of Application-Level Multicast Sessions. Pages: 141-146.

[33]. Bettahar, H., Alkubeily, M., Bouabdallah, A. (2007). Efficient Key Management Scheme for Secure Application-Level Multicast. Pages: 489-494.

[34]. Alkubeily, M., Bettahar, H., Bouabdallah, A. (2007). MDA - ALM: Membership Duration Aware Application-Level Multicast. Pages: 120-127.

[12]. Alkubeily, M., Ali, S., Raya, G. (2018). Scenario-Based Performance Evaluation for QoS Routing in MANET. Albaath University Journal, Vol.40.

[13]. Esber,Gh., and Alkubeily, M. (2018). Improving Secure Routing in Geographic Routing Protocols for Wireless Multimedia Sensor Network . International Journal of Computer Science Trends and Technology (IJCST), Vol.6, No.1, PP: 77-88.

[14]. Raya, Gh., Alkubeily, M., Ali, S., Maala, B. (2018). A New Multi-Objective QoS Multicast Routing Protocol Based on Ant Colony Optimization for Mobile Ad Hoc Networks. *International Journal of Computer Science Trends and Technology (IJCST)*, Vol.6, No.1, PP: 17-23.

[15]. Massoud, S., Ahmad, Y., Alkubeily, M., Ahmad, A. (2017). Reducing Energy Consumption in WBSNs using Statistic Test to detect Duplicated Data. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol.5, Issue.12, PP: 17608-17615.

[16]. Jbeily, Th., Hatem, I., Alkubeily, M., Challal, Y. (2017). Simple On-Line Single-View Video Summarization for Machine-to-Machine Wireless Multimedia Sensor Network. The 1st International Congress for the Advancement of Mechanism, Machine, Robotics and Mechatronics Sciences. (ICAMMRMS).

[17]. Alkubeily, M., Hatem, I., Jbeily, Th., Challal, Y. (2017). Symmetric-Object Oriented Motion Estimation Approach Test over Wireless Multimedia Sensor Networks for Different Motion Modes. Tishreen University Journal of Science and Engineering, Vol.39, No.6.

[18]. Alkubeily, M., Ali, S., Maala, B., Raya, G. (2017). A New Stable and Reliable On-Demand QoS Routing Protocol Based on Ant Colony Optimization for Mobile Ad-hoc Networks “, Tishreen University Journal of Science and Engineering, Vol.39, No.3.

[19]. Ahmad, A., Hammoud, O., Alkubeily, M. (2017). Increasing Patients' Privacy While Using Search Engines and Social Media Websites. International Journal of Science and Research (IJSR), Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391, Vol.6, Issue.7, PP: 2041-2045.

[20]. Hamoud, M., Hassoun, R., Mahmoud, A., Alkubeily, M., Ahmad, A. (2017). Comparison of MANET Routing Protocols Used in Home Health-Monitoring System for Elderly Patients. International Journal of Science and Research (IJSR), Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391, Vol.6, Issue.2, PP: 988-993.

[21]. Maala, B., Alkubeily, M. A New Fault Tolerance Protocol in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.38, No.6.

[22]. Jbeily, T., Alkubeily, M., Hatem, I. (2015). A New Symmetric-Object Oriented Approach for Motion

منشورات المؤلف (د. بشرى معلا):

[1]. Maala, B., Zarka, F. (2021). Blockchain Technology to a new View. Al-Manara University Journal, Vol.1, No.4.

[2]. Alkubeily, M., Maala, B. (2021). An overview of the Internet of Things-IoT. Al-Manara University Journal, Vol.1, No.1.

[3]. Maala, B., Alradwan, A., Mahfoud, A. (2020). Barycentric Jamming localization (BJL). Tartous University, Vol.4, No.8.

[4]. Maala, B., Alradwan, A., Mahfoud, A. (2020). Adaptive Detect and Protect Against Jamming Attacks on Ad Hoc Networks using Game Theory and Channel Switching (GTCS). International Journal of Computer Science and Technology IJCST, Vol.8, Issue.3, PP: 49-56.

[5]. Maala, B., Abd Alhameed, M. Studying the ARP spoofing attack effect on SDN networks. Tishreen University Journal of Science and Engineering, Vol.42, No.2, 2020. PP: 183-199 .

[6]. Maala, B., Alradwan, A., Mahfoud, A. (2019). Analyzing Study of the Effect of Jamming Attack on Ad Hoc Network Performance. Tishreen University Journal of Science and Engineering, Vol.41, No.5, PP: 81-98.

[7]. Maala, M., Mohammed, H. (2018). Enhanced Secure Data Aggregation in Mobile Wireless Sensor Networks. Tishreen University Journal of Science and Engineering, Vol.40, No.4, PP: 499-515.

[8]. Sweekat, Kh., Zarka, F., Maala, B., Ahmad, A. (2018). A New Secure Wireless Body Sensor Network Architecture. International Journal of Engineering Trends and Application (IJETA), Volume 5 Issue 1, PP: 41-45.

[9]. Raya, Gh., Alkubeily, M., Ali, S., Maala, B. (2018). A New Multi-Objective QoS Multicast Routing Protocol Based on Ant Colony Optimization for Mobile Ad Hoc Networks. International Journal of Computer Science Trends and Technology (IJCST), Vol.6, No.1, PP: 17-23.

[10]. Abo Ajeeb, A., Mahmod, A., Maala, B., Ahmad, A. (2017). Enhanced DNA Cryptography for Wireless Body Sensor Networks. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol.5, Issue 12, PP: 16953-16958.

[11]. Maala, B., Iskander, Kh. (2017). Performance Evaluation of MQQ- SIG Algorithm in Wireless Multimedia Sensor Networks. Tishreen University Journal of Science and Engineering, Vol.39, No.6.

[12]. Sliman, A., Madi, K., Khadour, A., Maala, B., Ahmad, A. (2017). Fabrication Attack Effect on Medical Applications based on VANETs. International Journal of Computer Science Trends and Technology (IJCST), Volume 5 Issue 2.

[13]. Maala, B., Mahfoud, A. (2017). Dynamic Black List (DBL) algorithm to defense against DDoS attack in Vehicular Ad-hoc Network. Tishreen University Journal of Science and Engineering, Vol.39, No.3.

[14]. Alkubeily, M., Ali, S., Maala, B., Raya, G. A New Stable and Reliable On-Demand QoS Routing Protocol Based on Ant Colony Optimization for Mobile Ad-hoc Networks. Tishreen University Journal of Science and Engineering, Vol.39, No.3.

[15]. Maala, B., Alkubeily, M. (2016). A New Fault Tolerance Protocol in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.38, No.6.

[16]. Hasan, B., Maala, B. (2016). Performance Evaluation for GPSR and AODV Routing Protocols at the Junctions in VANET. Tishreen University Journal of Science and Engineering, Vol.38, No.4.

[17]. Maala, B. (2016). Performance Study of APS Algorithm for position Determination in Underwater Wireless Sensor Networks. Tishreen University Journal of Science and Engineering, Vol.38, No.3.

[18]. Maala, B. (2015). Study of DDOS Attack Impact on Vehicular Ad Hoc Network in City. Tishreen University Journal of Science and Engineering, Vol.37, No.3.

[19]. Maala, B., Alkubeily, M. (2015). Fault Tolerance in Application-Level Multicast Networks. Tishreen University Journal of Science and Engineering, Vol.37, No.1.

[20]. Maala, B., Alkubeily, M., Raya, G. (2014). Improving Packet Delivery Ratio for On-Demand Multicast Routing Protocol (ODMRP). Tishreen University Journal of Science and Engineering, Vol.36, No.1, pp: 169-184.

[21]. Maala, B., Bettahar, H., Bouabdallah, A. (2010). Performances of Key Management schemes in Wireless Sensor Networks. Handbook on Sensor Networks. chapter 11, World Scientific Publishing Co.

[22]. Maala, B., Challal, Y., Bettahar, H., Bouabdallah, A. (2009). Node Capture Attack Impact on Key Management Schemes For Heterogeneous Wireless Sensor Networks. IEEE Global Information Infrastructure Symposium (GIIS).

[23]. Maala, B., Bettahar, H., Bouabdallah, A. (2008). TLA: A Tow Level Architecture for Key Management inWireless Sensor Networks. Pages:639-644.

[24]. Maala, B., Challal, Y., Bouabdallah, A. (2008). HERO: Hierarchical Key Management Protocol for Heterogeneous Wireless Sensor Networks. Proceeding of IFIP Conference on Wireless Sensors and Actor Networks (IFIP-WSAN'08), Pages:125-136.