Journal of Network and Computer Applications 66 (2016) 198–213

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Secure routing for internet of things: A survey

David Airehrour [a,*], Jairo Gutierrez [a], Sayan Kumar Ray [b]

[a] School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland, New Zealand
[b] Faculty of Business and Information Technology, Manukau Institute of Technology, Auckland, New Zealand

ARTICLE INFO

Article history:
Received 16 December 2015
Received in revised form
17 February 2016
Accepted 8 March 2016
Available online 10 March 2016

Keywords:
IETF
6LoWPAN
RPL
IEEE 802.15.4
IoT
Routing
Security
Sensors

ABSTRACT

The Internet of Things (IoT) could be described as the pervasive and global network which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. It is projected that by 2020 the number of connected devices is estimated to grow exponentially to 50 billion. The main drivers for this growth are our everyday devices such as cars, refrigerators, fans, lights, mobile phones and other operational technologies including the manufacturing infrastructures which are now becoming connected systems across the world. It is apparent that security will pose a fundamental enabling factor for the successful deployment and use of most IoT applications and in particular secure routing among IoT sensor nodes thus, mechanisms need to be designed to provide secure routing communications for devices enabled by the IoT technology. This survey analyzes existing routing protocols and mechanisms to secure routing communications in IoT, as well as the open research issues. We further analyze how existing approaches ensure secure routing in IoT, their weaknesses, threats to secure routing in IoT and the open challenges and strategies for future research work for a better secure IoT routing.

1. Introduction

With the advancement in mobile computing and wireless communications, a new paradigm known as the *Internet of Things* (IoT) is swiftly generating a lot of research interest and industrial revolution. The *Internet of Things* (IoT) could be described as the pervasive and global network, which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. These devices have built-in sensing and communication interfaces such as sensors, radio frequency identification devices (RFID), Global Positioning devices (GPS), infrared sensors, laser scanners, actuators, wireless LANs and even Local Area Networks (LANs) interfaces (Zhao and Ge, 2013). These "*things*" can be connected to the internet and hence could be controlled and managed remotely. These devices could interact among themselves (Machine-to-Machine (M2M)) by way of sending and receiving information, sensing the environmental temperature, pressure etc. while transmitting same to other devices for further processing or other actions (Xu et al., 2013; Wei and Qi, 2011). According to International Telecommunications Union (ITU) and the *IoT European Research Cluster* (IERC) the Internet of Things (IoT) is defined as a vivacious worldwide network infrastructure with self-configuring capabilities centered on standard and interoperable communication protocols in which physical and virtual "things" have identities, physical features and virtual characteristics, communicate via intelligent interfaces and integrate into the information network in a seamless fashion (Fig. 1).

IoT can be viewed as a fusion of heterogeneous networks that brings not only the same security challenges present in sensor networks, mobile telecommunications and the internet but also some peculiar and accentuated issues, like, network privacy problems, authentication on a heterogeneous network, access control challenges and secure routing among these heterogeneous devices (Zhao and Ge, 2013).

The IoT has, in the last few years, become a topical issue in academia and industry. While becoming increasingly ubiquitous, IoT supports a comprehensive representation of the physical environment and a good level of interaction with the physical world (Atzori et al., 2010; Gubbi et al., 2013). Areas such as logistics, intelligent transportation systems (ITS), business/process management and e-health are just few instances of conceivable application fields where this novel paradigm will be highly useful. The realization of IoT will greatly hinge on various criteria such as the system's architecture, networks and communications, data processing, and ubiquitous computing technologies which support efficient, reliable, physical and cyber interconnectivity. A fundamental driving force of IoT that facilitates the interconnection of devices is networking, and specifically, routing in the network. It involves the creation of traffic routes, and transmitting the routed packets from source to final destination in a network. With billions

* Corresponding author.

http://dx.doi.org/10.1016/j.jnca.2016.03.006
1084-8045/

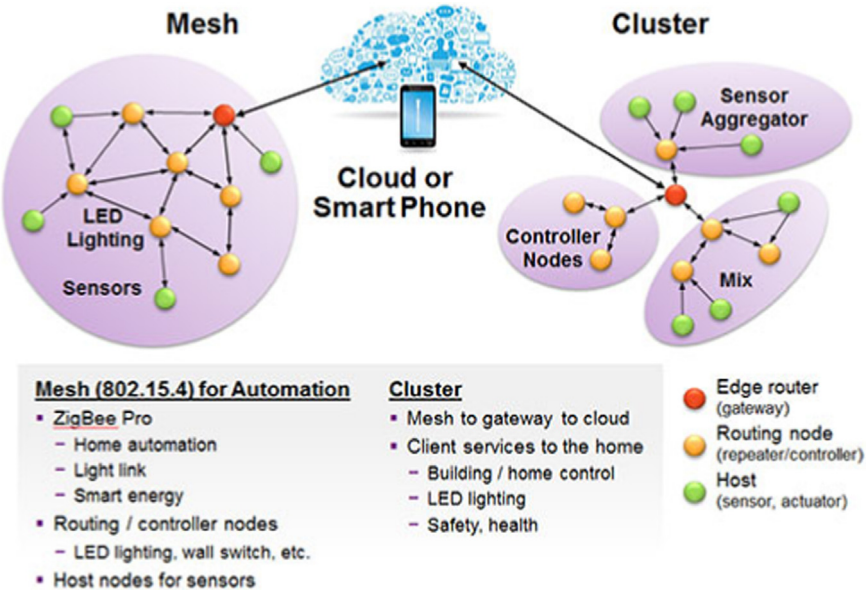

Fig. 1. An interconnectivity of IoT nodes comprising of edge routers (gateway to the cloud), routing nodes (that also serve as control nodes) and mobile sensory or actuator nodes (Spansion, 2014).

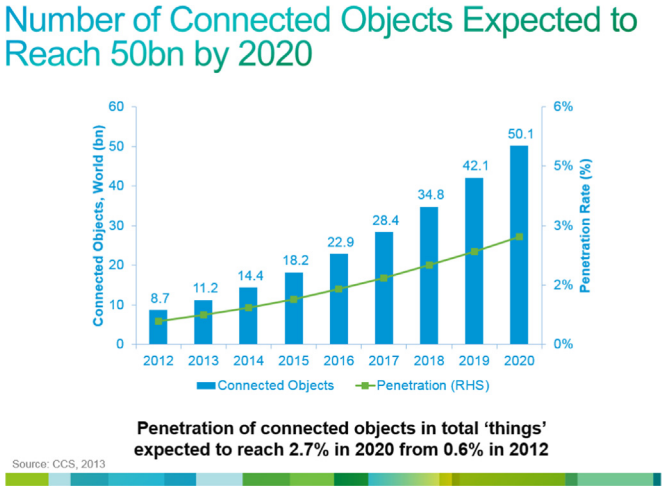

Fig. 2. A forecast of more than 50 billion interconnected devices by 2020: Source (CISCO, 2013).

of devices interconnected in the network, an uphill challenge is securing the network from various forms of threats and attacks. Users will feel insecure about their private data if they are vulnerable to attacks from unauthorized individuals or machines over the network. With 50 billion interconnected IoT nodes, as shown in Fig. 2, security is by far one of the biggest challenges in IoT networks (Evans, 2011; Ericsson, 2011; CTIA-The Wireless Association, 2014).

Sequel to our discussions above, routing and addressing are critical issues in IoT owing to the requirement of maintaining a uniformity in the way packets are routed between source and destination between IoT devices traveling across varying network topologies. Making the process of routing secure enough in IoT is even more challenging (Gubbi et al., 2013). This imperative need for securing the routing process between numerous IoT devices across multiple heterogeneous networks needs significant research contributions. Current research findings show that IT security threats for 2013–2015 are threats that subsist only with the presence of a network and they include: botnets, malware, Denial-of-Service (DoS) attacks on financial services and Distributed Denial of Service (DDoS) attacks, web-based malware, android malware and Spam (Mc Afee Labs, 2014; Sophos Limited, 2013, 2014).

In this survey, we explore the IoT routing protocols in general and discuss few of the key secure IoT routing protocols and their vulnerabilities to attacks during routing. The contribution of this paper is threefold. First, we introduce the Internet of Things and its relevance as well as growing trends in today's global IT scenario. Second, the paper gives an overview of the threats associated with IoT routing and identifies few of the research challenges as discussed by the research fraternity. Lastly, the paper briefly highlights some of the potential research directions in achieving secure and sustainable routing among IoT devices. To the best of our knowledge, this survey paper is the first of its kind intending to provide researchers and readers a broad overview on the different research findings and proposed solutions on the issue of secure routing among IoT devices. The rest of the paper is organized as follows. Section 2 briefly talks about the security and energy consumption in IoT networks. The routing protocols are discussed in Section 3. This is followed by Sections 4 and 5 that, respectively, discuss the vulnerabilities to IoT routing and trust in IoT secure routing. An overview of the issues and challenges of secure routing in IoT is provided in Section 6 and finally, in Section 7 we conclude the survey.

2. Security and energy consumption: where the need lies in IoT?

IoT has many promising areas of application including commercial (oil well sensing, intelligent vehicular transportation system, gaming, and agriculture), smart homes, wearables, healthcare, automotive industries and the power smart grid system. To maintain the seamless functioning of the IoT networks, the areas of primary focus in IoT research are the (a) security (including the communication between sensor nodes) and (b) energy consumption of the different IoT nodes. In the following sub-sections, we explore these two aspects that will play key roles in the IoT revolution.

2.1. Security in IoT

IoT exhibit unique characteristics, which requires security while in operation to protect the network from various attacks. The fundamental requirements ensuring the security of any IoT network remain a challenge. To achieve the goal of having a secure IoT network, there are however, important features or properties that must be considered to have a secure IoT network as specified by Mishra (2008) and Parker (1991):

Availability: Availability is the provisioning of network services at all layers of a network to all nodes while ensuring the survivability of all network services even in the presence of malicious attacks. Since IoT will be employed in crucial and important areas of the global economy, security in the aspects of availability and dependability will be of top priority.

Authenticity: A process whereby nodes are required to identify themselves and prove their identities on the network. This is needful in order to protect the security of the network from impersonating nodes who could disrupt the network or gain access to vital information and hence, disrupt the network system. Since many nodes will be communicating in a heterogeneous fashion, node authentication is necessary to avert illegal node access in IoT network.

Confidentiality: Confidentiality guarantees information does not get divulged to the wrong source. In ad hoc networks, it ensures malicious nodes do not gain unauthorized access to vital routing or data information either from any legitimate node or while such information is in transit. Confidentiality imposes a prohibition on untrusted nodes from comprehending and accessing the content of vital data being communicated. In IoT, in order to protect the confidentiality of information transmission between the nodes, routing and data encryption is important so as to provide stronger safety measures during network communication.

Integrity: This is the assurance that data received by a destination node has not been changed in transit either through collision or via a deliberate tampering by an untrusted node while in transit. The data received should be as originally sent. In some instances, data packets could suffer from collision due to radio wave propagation; however data packets could still be modified by untrusted nodes in order to disrupt the network. In IoT networks, data integrity should be embedded in the design since an IoT device collects, stores, sends, and shares data according to a given protocol standard.

Non-repudiation: Non-repudiation involves a source node owning up to data it has sent while a receiving node acknowledges receipt of the same. Neither party can deny knowledge of either sending or receiving the information. Non-repudiation is essential in detecting and isolating untrusted IoT nodes that may seek to send false network information while seeking to deny they ever sent such information.

IoT uncovers new aspects of security challenges in the underlying network topology. Owing to the heterogeneity of IoT networks, they are more susceptible to malicious attacks than wired networks. The vulnerability of communication channels and nodes along with high mobility of the underlying changing topologies make IoT security a daunting task to deal with. Issues like eavesdropping, wireless broadcast of messages and injection of false information into the network greatly compromise the integrity of IoT communication. Moreover due to the constrained nature and self-organizing attribute of IoT sensor nodes, the use of a solution centered on certification authorities (CA) via connected servers poses extreme difficulty for secure routing among IoT nodes (Sarkar et al., 2013; Pervaiz et al., 2005; García-Teodoro et al., 2014; Wei et al., 2014). Since IoT networks are exposed to various attacks, securing them poses great difficulty (Chugh et al., 2012).

According to Gartner (2014), by 2020 the number of interconnected IoT devices is expected to reach 25 billion and further research from HP highlighted that on an average there are approximately 25 vulnerabilities per IoT device, which accentuates the requirement for better IoT security (Packard, 2015). Here we summarize the findings from HP:

i. *Privacy issues*: Huge number of IoT devices gather sensitive and private information, like name, address, and insurance policy number etc., of users. An example is in the health sector where IoT nodes collect and transmit some form of personal information such as name, address, date of birth and health statistics. These concerns become even more accentuated when these details are now transferred and deployed unto the cloud using mobile applications, which work with these IoT devices. Transmission of this ultra-sensitive information across the IoT networks, without adequate security measures, is a huge concern, as it is possible for unauthorized personnel to access the information.
ii. *Inadequate authentication/authorization*: HP surveyed multiple IoT devices (webcams, TVs, home thermostats, remote power outlets, home alarms, door locks, garage door openers, and scales) present in the market and found out that they either do not require strong passwords for accessing them or may have poor password recovery systems. Not only that, a number of such devices utilize similar insecure passwords on their websites and/or mobile applications, enabling a possibility for potential malicious software to remotely gain control of them.
iii. *Absence of transport encryption/standard*: The HP research showed that most of the devices did not encrypt network transmission for both local network data and the Internet. This is due largely to the lack of standardization in the IoT framework. Since these IoT devices collect and transmit confidential data it is imperative for transport encryption systems to be in place while transmitting data over IoT network.
iv. *Web interface vulnerability*: This is a security vulnerability in web applications used by hackers to circumvent access controls. In their report, they identified recurrent cross-site scripting, vulnerable weak sessions and poor credentials management as severe security issues. Bearing in mind that most of these devices provide access through the cloud, these become notable security issues.
v. *Software and firmware vulnerability*: As identified by HP, more than 60% of the IoT devices have software and firmware vulnerabilities present in them resulting from lack of encryption standards while upgrading the software and firmware. This proves that malicious software and firmware could gain remote access to these devices through system updates (Fig. 3) summarizes the above-mentioned findings of HP.

Privacy preservation for IoT devices and users is another key issue in IoT. Even with the existing authentication approaches and cryptographic mechanisms in place to safeguard users' privacy in IoT networks, issues like heterogeneity of IoT networks, limited battery capacity of devices and the devices' resource constraints in terms of available memory cripple the communication. As a result, multiple devices in IoT network end up not utilizing in an optimal manner the available authentication and cryptographic mechanisms. This clearly shows the need for better secure systems for the IoT networks. The US Federal State Commission (FTC) identified this and have announced the need to secure the IoT ecosystem after security violation was reported for the TRENDNet IP camera in 2012 where live footage from thousands of TRENDNet security cameras have been penetrated, permitting web users to access live video footage without requiring any password (Smith, 2013).

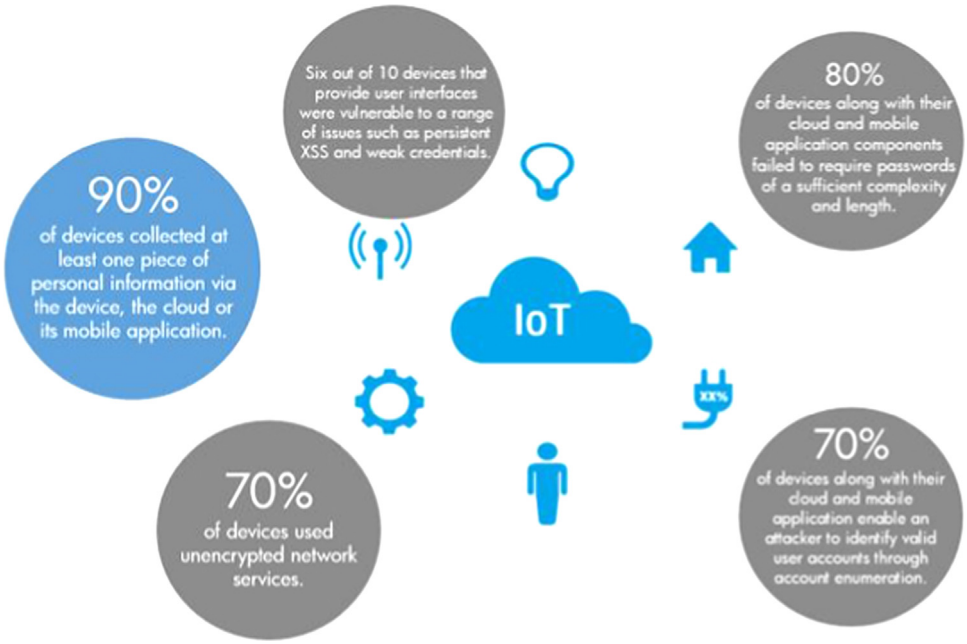

Fig. 3. Security Vulnerability of IoT devices (Packard, 2015).

Similarly, such security requirements have also been reported by the European Union Data Protection WP29 committee (EU, 2014).

Generally speaking, security threats in IoT networks could be classified into the following two groups. *(a) General security threats in IoT networks:* Such threats are comparable to those occurring in traditional network systems because of issues like confidentiality, integrity, and availability (CIA) and they include DoS attacks, man-in-the middle-attack (MITM). However, owing to the massive size, complexities and magnitudes of IoT networks along with the heterogeneity of the underlying communication networks and nodes, the threats pose much bigger challenges than traditional network systems. *(b) IoT specific security threats:* This is largely because of the massive interconnectivity of different types of IoT devices and the heterogeneity of the underlying networks. These threats are specific to the ways IoT systems interact with our daily lives. For example, data gathered while measuring and exchanging sensitive private data, like a patient's medical readings (e.g., heart beat rate, blood pressure, temperature) or smart meter readings or eco-forest readings over the IoT communications network could be compromised. The data may be hacked and maliciously transmitted to rogue IoT nodes as a result of a network route attack.

IoT is still in its nascent phase and having appropriate security measures, probably in the form of a framework is imperative to address the conglomerate of security challenges that may inhibit this disruptive technological revolution. The framework should define proper information gathering mechanisms from the associated IoT devices/nodes, proper data privacy definition system, and further take into account the type and nature of underlying communications between the connected devices for which limited energy is a constraint. Albeit, such a framework can be useful for IoT networks as it may help in protecting private data from being compromised by rogue and malicious nodes while giving users the assurance that their information is not being divulged to the wrong party.

2.2. Energy consumption in IoT

Most IoT nodes are typically battery powered and that makes energy efficiency critical for proper functioning and management of these nodes. Energy efficiency and sufficiency in IoT sensor nodes have been active research areas (Shibo et al., 2012; Gu et al., 2013; Yoo et al., 2015). The Medium Access Control (MAC) layer protocols in IoT networks concentrate on regulating the duty cycle of sensor nodes and the network layer protocols are focused on data aggregation designs and multipoint-to-point transmission. For battery powered IoT nodes, regular battery monitoring is essential since the nodes operate in the IoT network platform. For more details on this we refer readers to (Yoo et al., 2015). IoT nodes have limited energy and communication between the different nodes is energy consuming. Efficiently connecting the different energy constraint nodes while optimizing the limited energy in them remains a fundamental challenge in IoT communication (Shibo et al., 2012; Gu et al., 2013). Many low-powered communication technologies are developed and considered today as enabling technologies for IoT. These include, technologies enabling “things” acquiring contextual information, technologies enabling “things” processing contextual information, and technologies improving security and privacy.

From the survey of different literature (Shibo et al., 2012; Gu et al., 2013; Yoo et al., 2015), it is quite clear that a key cause of energy drains on IoT nodes is the RF communication component. Various communication metrics-related trade-offs are explored and a number of solutions for optimization of energy consumption are proposed which considers the general communication requirements and patterns specific for different application classes (Shibo et al., 2012; Gu et al., 2013; Liu et al., 2013; Miller and Vaidya, 2005; Cheng et al., 2009). The energy source of an IoT sensor node can be influenced by factors associated with the node's reliability and its mode of operation. Batteries, although are a good source of power, they have a specific life cycle period that limit their usage up to a certain time. However, regularly replacing batteries for a large number of IoT nodes may prove expensive, daunting and impracticable in many cases due to the large number of nodes and their remote locations.

In context to the above discussion, it may prove effective to have factory-enabled batteries in the nodes (like a small form factor battery) that will last the entire lifetime of the nodes. This will not only reduce IoT application costs but, will also arguably improve the service reliability. Effectively, this will offer more computation ability and reduced energy consumption at a lower

cost. Other evolving areas of low power technologies for sensor nodes exist and they have the capability of providing energy efficiency and self-sufficiency to IoT sensor nodes. They include ambient, solar, and thermoelectric.

IoT sensor nodes may as well benefit from energy harvesting technologies, like, vibration or electromagnetic radiation, ambient light, thermal energy, that have the capability to provide much enhanced power to the nodes. A sensor node's basic components include, a sensor microcontroller, a power harvesting transducer, an energy conversion system, and the wireless radio used for communications. Thus, for such nodes to optimally benefit from energy harvesting, there is a need to have an efficient power conversion system, energy storage system, and power management system. On the flip side, specifically speaking of ambient energy sources, their specialized requirements for deployment may cause the overall applications costs to go up (Vermesan and Friess, 2014).

3. Routing protocols in IoT

One of the fundamental aspects of the Internet of Things is the manner low powered devices self-organize and share information (route and data information) among themselves. Even though these sensory devices are energy constrained, they however, perform storage and computation functions while communicating over lossy channels. These nodes work in unison and can join and leave the network at any time. It is of importance that the wireless routing solution for these sensor networks should be scalable, autonomous while being energy-efficient. The devices utilized in these low power lossy networks (LLN) are basically sensors and actuators but they have routing capabilities. Some of these sensor nodes act as border routers and hence connect the LLNs to the internet or to a closely located Local Area Network (LAN). Such routers are commonly referred to as LLN border routers (LBR) (Ishaq et al., 2013; Machado et al., 2013). Fig. 4 illustrates a layered IPv6 architecture of an end-to-end connectivity covering a field area network.

3.1. IoT routing protocols

The Internet Engineering Task Force (IETF) created working groups (WGs) which developed various IoT protocols for IoT devices. We present below a description of the IETF protocols which have been developed for the Internet of Things (IoT) and a review of the weaknesses inherent in these protocols.

3.1.1. IPv6 over low power wireless personal area networks (6LoWPAN)

6LoWPAN is an IETF-standardized IPv6 adaptation layer (data link and cross-layer protocol) that enables IP connectivity over low power and lossy networks (Winter et al., 2012; Watteyne et al., 2009). This is seen as the foundation for the network build up for the Internet of Things such as smart homes, smart cities and industrial control systems (Watteyne et al., 2009). A large number of applications utilize 6LoWPAN for IP-based communication through an upper layer protocol such as the RPL routing protocol. 6LoWPAN essentially adjusts IPv6 packets into frames of 127 bytes – a frame size requirement that low power sensor devices can utilize among themselves. Also, 6LoWPAN supports the transmission of large-sized IPv6 packets on the data link layer of the IEEE 802.15.4. It further provides fragmentation support at the adaptation layer although, the system of fragmentation makes processes such as buffering, forwarding and processing of fragmented packets resource expensive on these already resource constrained devices. Rogue nodes can send duplicate, overlapping or stale fragments to disrupt the network. A security breach can be seen in this layer as there is no authentication at the 6LoWPAN layer, hence receiving nodes are incapacitated in differentiating between legitimate and spurious packets during fragment re-assembly. Receiving nodes during re-assembly normally store up the fragments received in order to re-assemble them. If the entire set of frames making up the packet are not received after a certain timeout they are discarded. This system could also be exploited by malicious nodes which could send fake fragments to fill up the node's store so, it does not receive the legitimate fragments for re-assembly. This is indeed a challenging security issue in IoT networks (Hummen et al., 2013). However, some protocols which have adopted 6LoWPAN (Winter et al., 2012; Hui and Thubert, 2011; Shelby et al., 2012) hinge on the security sublayer of the 802.15.4 to prevent 802.15.4 frames introduced by malicious nodes. Indeed the 802.15.4 security sublayer actively achieves this aim by adding to every frame a Message Integrity Code (MIC) and a frame counter. The design of an 802.15.4 includes an unspecified key for security purposes though the purpose of the key is uncertain thus utilizing this key to preload each node with a shared-key for the network exposes the nodes to network attacks. An attacker could physically interfere with a node in order to

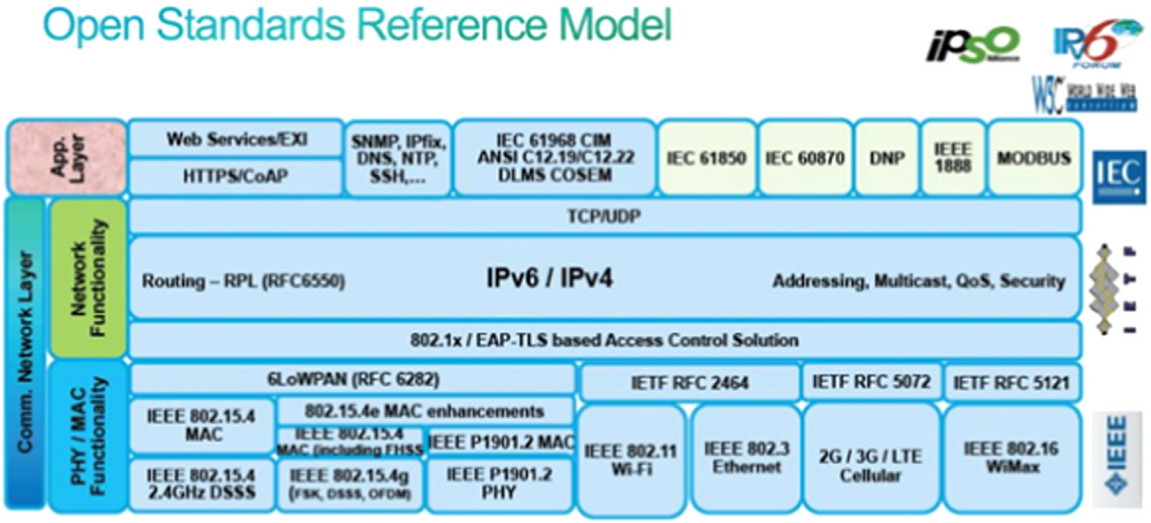

Fig. 4. A Layered IPv6 architecture showing end-to-end connectivity covering a field area network: Source CISCO.

decipher its cryptographic details. Tamper-resistant hardware could be used to forestall this type of attack (Becher et al., 2006), but it comes at a high cost even though it does not guaranty absolute security (Anderson and Kuhn, 1996). Once a node has been compromised the attacker could easily inject spurious frames into the network and thus, add other non-authorized nodes into the victim's network. This error and security loophole could be propagated even to the upper layer of protocols since, the upper layer protocols rely on the 802.15.4 security sublayer for the security of frames (Winter et al., 2012; Shelby et al., 2012).

3.1.2. Routing protocol for low-power and lossy networks (RPL)

RPL was developed by the IETF working group [ROLL WG] as routing functionalities in 6LoWPAN were very challenging due to the resource constrained nature of the nodes. RPL operates at the network layer making it capable to quickly build up routes and distribute route information among other nodes in an efficient manner (Anhtuan et al., 2013). RPL is a Distance Vector IPv6 routing protocol for LLNs, thus network path information is organized as a set of Directed Acyclic Graphs (DAGs) and this is further classified as a set of Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG typically consist of sensor nodes and a sink node which collects data from these nodes as shown in Fig. 5. Every DODAG is distinguished by four factors which include: DODAG ID, DODAG version number, RPL instance ID and Rank while every DODAG sink is linked with each other (Winter et al., 2012). Route selection in RPL depends on the DODAG link, cost of information to a node such as workload, throughput, node power, latency or reliability.

To produce a route topology, every node selects a set of parents that comprises nodes with equal or better paths towards the sink. The node with the best route link is chosen as the parent. RPL employs three types of control messages in order to form and manage routing of information in the network and these are:

i. DODAG Information Object (DIO), used for setting and updating the network topology.
ii. DODAG Advertisement Object (DAO) used for broadcasting and advertising destination information upwards during network route updates.
iii. DODAG Information Solicitation (DIS) used when a new node seeks topology information while waiting to join the network.

DAO and DIS are involved during a topology change process while the DIO message is broadcast and mainly used for the purpose of starting a topology change process. DIO is commonly used to distribute its routing state to other nodes using its rank (rank specifies the link quality to a sink node) and objective function (Winter et al., 2012; Anhtuan et al., 2013). Every node computes its rank according to the rank of its selected parent and the objective function. A DIO message is sent to all nodes every time a node updates its rank or preferred parent. To prevent the formation of loops, RPL utilizes the rank rule whereby a node in a parent should always have lower rank than its children. Also, to limit the amount of broadcast, RPL uses the trickle algorithm for scheduling DIO messages to be sent. It does this by setting a counter which observes the network topology and thereby decide when a node has to send a DIO message. For every DIO message received without comparing it with the previous DIO message this will cause the DIO counter to increase and if the DIO counter reaches a threshold value (redundancy value) the node will reset its DIO counter and double the trickle time. This is done to stabilize the network topology over a period of time and avoid the unnecessary frequent route updates which could consume the limited power and bandwidth available. This further helps to limit the number of DIOs produced so as to preserve scarce network resources. For incoming traffic, the node resets its DIO to zero and reduces its trigger time. This gives the opportunity for quick network route update through a rapid DIO generation (Winter et al., 2012).

The RPL routing protocol has capacity to incorporate different types of traffic and signaling information swapped among nodes although this depends on the requirements of the considered data flows. RPL supports the Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP) and Point-to-Point (P2P) traffics (Evans, 2011; Yashiro et al., Sakamura).

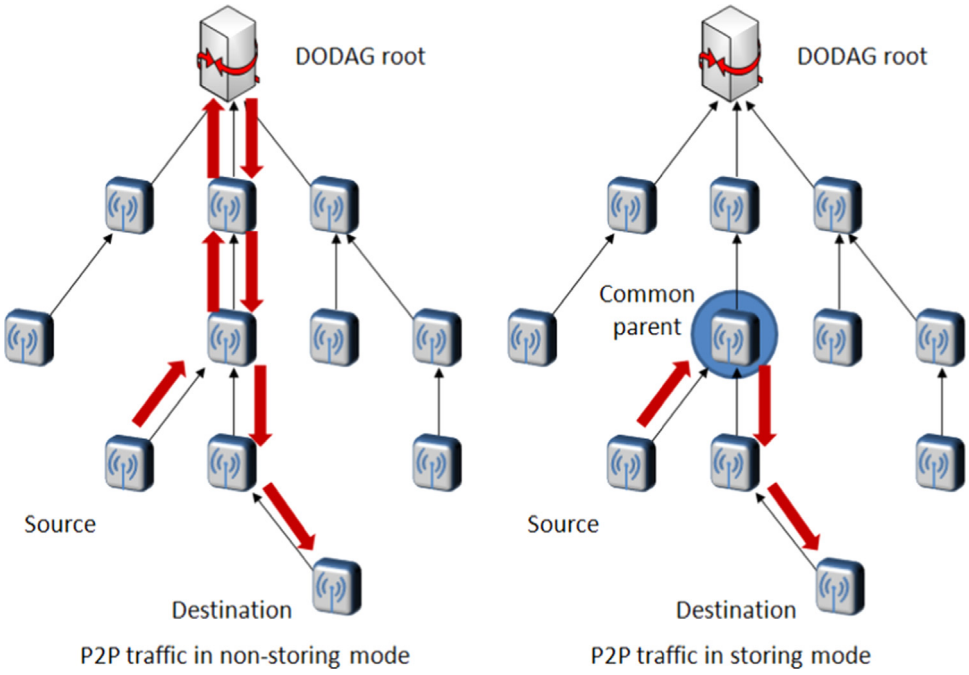

Fig. 5. An RPL network showing the flow of packet in a point-to-point traffic between two nodes.

The rank property is central to the efficient routing operations of the RPL routing protocol. The rank property helps to manage control overhead, prevent loop formation and create optimal network topology. So any attack at the rank property will severely disrupt the proper functioning of the RPL protocol. RPL presumes nodes in the network are consistent and follow the protocol rules thus, it does not provide a system for examining consistent node behavior and this creates the opportunity for malicious nodes to attack the rank property (Anhtuan et al., 2013). RPL is also susceptible to the HELLO message attack. This is a broadcast message a node sends out when trying to join a network. These malicious nodes usually have strong broadcast signal to reach other nodes and broadcast a perceived good routing metric. A malicious node advertises itself and when the nodes seek to align with it, their request messages get lost because they are out of range from the malicious node. And this continues until the legitimate nodes exhaust their battery power in trying to connect with the malicious node. DIO messages used to advertise DODAGs information could be used by these malicious nodes to succinctly launch HELLO flood attacks although with link-layer security turned on this could be averted. However, malicious nodes realizing this try to compromise one of the legitimate nodes in the network in order to still launch out the hello flood attack (Wallgren et al., 2013). Again, another attack RPL is susceptible to is the sinkhole attack. The RPL protocol gives numerous details to nodes in the DODAG in order to determine the node that will act as the default route. One such detail is the rank, this is computed and sent out to the neighboring nodes from the DODAG root. A malicious node simply advertises a better rank to other nodes thus, attracting nodes to itself in order to become their parent in the DODAG. Even though RPL uses the link-layer quality to compute routes, this makes a sinkhole attack less effective in RPL but the attacks are still possible (Anhtuan et al., 2013; Wallgren et al., 2013).

3.1.3. IPv6 over the time slotted channel hopping mode of IEEE 802.15.4e (6TiSCH)

The development of this IoT protocol is currently ongoing and has not being deployed yet. It will be based on IPv6's multi-link subnet spanning over high speed IEEE 802.15.4e TiSCH wireless mesh networks linked to the backbone via synchronized backbone routers (Evans, 2011; Yashiro et. al, 2013). The new protocol will include details about how packets, belonging to a deterministic IPv6 flow, may be treated while issues such as classification, routing and forwarding of packets over the mesh network can be addressed. Other areas to be addressed will include security, link management for the IPv6 network layer, neighbor discovery and routing [6tiSCHesIoT] (Yashiro et. al, 2013; IETF, 2014).

4. Vulnerabilities to routing in IoT

IoT is firmly based on the use of the IPv6 addressing scheme. This makes it exposed to the same attack threats as IPv4, such as black hole attacks, reconnaissance, sybil, spoofing, smurfing, eavesdropping, neighbor discovery, man-in-the-middle, rogue devices and fragmentation attacks etc. This clearly demands the same security measures been used today for IPv4. In addition, since IoT is envisioned as the intersection of where the Internet meets with the physical world, it further unlocks a whole new plethora of security concerns. This creates a number of serious security implications whereby attack threats will shift from manipulating information to the actual control of actuating devices i.e. moving threats from the cyber world to the physical world. Accordingly, this radically creates a wide and fertile attack surface from well-known threats and devices, to the added security threats of new devices, protocols, and workflows as more and more electronic systems are being ported from closed systems (such as Modbus, SCADA) into IP-based systems and this will further increase the risk of more attacks.

4.1. Threats related to routing protocols

For a route to be established in a wireless mobile network, route information is transmitted from node to node (multi-hopping) until the desired destination is found. All throughout the route maintenance phase the nodes can add, delete or needlessly delay the transmission of control information (selfish or misbehaving nodes). It is during this route discovery or route forwarding that malicious nodes perpetrate their activities, thus several types of attacks are possible in the routing of information. As an example, a node can introduce a *routing table overflow attack* by transmitting a large amount of false route information to its neighbors in a manner that will cause its neighbor's routing table to overflow. This action causes the neighbor's routing table to be occupied by spurious routes and hence, denying the real routes from been captured in the routing table. Also, malicious nodes can advertise fabricated routes for neighbor nodes to update their routes in order to poison the routing cache. In AODV which is an ad hoc routing protocol, a malicious node can advertise a false route with the smallest hop count and with the latest sequence number, hence other nodes seeing this as a route update quickly invalidate their old route to accept innocently the new false route. Furthermore, in the route maintenance phase, a malicious node can transmit false route error messages which can trigger the start of a costly route maintenance process (Islam and Shaikh, 2013).

IoT networks require adequate security for a seamless operation and also for the public to build confidence in this new and emerging disruptive technology. The data communication among IoT devices could be achieved based on an end-to-end or on a hop-by-hop basis. The deployment of IPsec (Raza et al., 2011; Hennebert and Dos Santos, 2014) could provide end-to-end security between two communicating IoT hosts. In 6LoWPAN which is an IoT protocol, IPsec is enabled which could be used for secure communication among IoT hosts since the Encapsulating Security Payload (ESP) of IPsec's protocol (Kent, 2005a) could guarantee the confidentiality, integrity and authentication of data while the Authentication Header (AH) (Kent, 2005b) protocol ensures the integrity of the entire IPv6 datagram which consists of the application data and IPv6 headers. As an example, the Constrained Application Protocol (CoAP) (Shelby et al., 2011) employs an end-to-end security among two communicating host-based applications which uses the Datagram Transport Layer Security (DTLS) while the IEEE 802.15.14 link-layer security could be implemented for per hop security. Despite the security provided for data communication at the higher layer and the provision of link-layer security, the network layer of the IoT lays bare to routing attacks as there are no security standards defined at this layer (Wallgren et al., 2013).

In IoT networks like WSNs and MANETs, have similar attributes and thus face similar routing attacks such as the blackhole attacks, sinkhole attacks among others. A comprehensive study on these attacks have been covered by Islam and Shaikh (2013), Wu et al. (2007), Gagandeep and Aashima (2012), Singh et al. (2010), Hamid et al. (2006), Sanzgiri et al. (2005), Awerbuch et al. (2002), Hu et al. (2003), Yih-Chun et al. (2005) and Wei et al. (2012). We present in Table 1 a summary of attacks in RPL and countermeasures.

4.2. Secure routing protocols in IoT

In preventing routing attacks, several secure routing strategies have been proposed in the literature. In this section, we present an overview of the different secure routing protocols proposed by the

Table 1
Summary of RPL attacks and countermeasures.

Attacks	*Classification of attacks*	*Effect on network performance*	*Proposed protocols addressing attacks*
Rank	Confidentiality & Integrity	Low packet delivery ratio and packet delay; generation of non-optimal path and loop	Use of IDS based solutions (Raza et al., 2013), (Amin et al., 2009), VeRA (Dvir et al., 2011), TRAIL (Perrey et al., 2013)
Selective forwarding	Confidentiality & Integrity attack	Disruption of route path	Heartbeat protocol (Wallgren et al., 2013)
Sinkhole	Confidentiality & Integrity attack	Compromising huge traffic passing through attacker node	IDS solution (Raza et al., 2013), Parent fail-over, rank authentication technique (Weekly and Pister, 2012)
Hello flooding	Availability attack	Dissipation of sensor battery power	RPL's global and local repair mechanism removes attack
Wormhole	Confidentiality & Integrity	Disruption of route topology and traffic flow	Markle tree authentication (Zhang et al., 2014)
Sybil and Clone ID	Confidentiality & Integrity attack	Route compromise and traffic unreachable to victim's node	Routing attacks and countermeasures in RPL-Based IoT (Wallgren et al., 2013)
Denial of Service	Availability attack	Resources unavailable to nodes	Intended user IDS based solution (Kasinathan et al., 2013)
Blackhole	Availability, Confidentiality & Integrity	Dropped packets and increased route traffic and control overhead	SVELTE (Raza et al., 2013) Monitoring of counters (Chugh et al., 2012), Parent fail-over (Weekly and Pister, 2012),
Version number	Confidentiality & Integrity	Increased control overhead and low packet delivery ratio, high end to end delay	VeRA (Dvir et al., 2011)
Local repair Control overhead	Confidentiality & Integrity	Control and routing traffic disruption	IDS based solution (Le et al., 2012)
Neighbour attack	Confidentiality, Integrity & Availability	False route, route disruption and resource consumption	TRAIL (Perrey et al., 2013)
DIS attack	Availability	Resource consumption	TRAIL (Perrey et al., 2013)

research fraternity. This is followed by a presentation in Table 2 that summarizes secure routing protocols in IoT and Table 3 which provides a comparative study in context to the relative complexities, scalabilities and evaluation of the surveyed protocols.

i. *Secure multi-hop routing for IoT communications:* The work described in Chze and Leong (2014) introduces a secure multi-hop routing protocol (SMRP) which allows IoT devices to communicate in a secure manner. It achieves this by making sure that IoT devices authenticate before they could join or create a new network. The routing protocol proposed incorporates a multi-layer parameter into the routing algorithm and hence, when nodes want to join the network, they have to authenticate. The authors claim this protocol comes with no additional overhead on the routing process as the multi-layer parameters contain the permissible applications on the network, a unique User-Controllable Identification and a summary of devices allowed on the network. It can however, be seen that there will be much overhead in creating a multi-layer parameter that will host even as few as 100,000 IoT nodes in this type of network. This makes this protocol unusable on a large scale.

ii. *TSRF: A trust-aware secure routing framework in wireless sensor networks:* The trust-aware secure routing framework (TSRF) (Hummen et al., 2013) designed for WSNs was based on trust derivation which consists of direct and indirect observations of behavioral patterns of sensor nodes with trust values among nodes represented in a range from 0 to 1. A 0 signifying no trust exists between nodes and a 1 showing a good level of trust for the corresponding node. The authors opined that their system addressed the following attacks: on-off attack, conflicting behavior attack, selfish attack, bad mouthing attack and collusion attack. However, TSRF expended significant amount of memory due largely to the complex trust computations among the nodes. Also, rogue nodes were identified based on previous trusts among one another which revealed that a new rogue could join the network and behave well for a while and earn a good history. After earning this good history of trust they begin to carry out their malicious behavior within the network.

iii. *Two-way acknowledgment-based trust (2-ACKT)* (Anita et al., 2013): This system operates in a non-promiscuous mode and is contingent only on direct trust between nodes. The scheme is based on a dual acknowledgment system in developing trust among neighboring nodes. The scheme further develops a route to the sink node as well as introduced a new node (regarded as the sponsor and third party node) which creates a two hop acknowledgment in the network. One basic assumption the protocol makes is, that all malicious nodes drop data packets and not the acknowledgments hence, it cannot isolate greyhole attacks. Also, since the neighboring nodes were not the source of the recommendations, it follows that the conclusions on trust relationships might not be in consonance with the state of the network.

iv. *The group-based trust management scheme (GTMS):* The Group-based trust management scheme (GTMS) was proposed by Krentz et al. (2013) which is a trust based scheme involving the computation of trust via a direct observation among nodes i.e. the number of successful and unsuccessful interactions among nodes. The authors defined successful interaction as *positive collaboration* among nodes and *indirect observation* (recommendation of trusted peers concerning a node in the network) among nodes. Cluster Heads (CH) were created at the intra-group level and a distributed trust management scheme was used for gathering recommendations from all its group members and also about other CHs directly from the sink. The trust level was defined using unsigned integers from 0 to 100 so as to decrease memory usage. Even though the system addressed black hole attacks, the cluster heads at the intragroup level had a high energy requirement for them to communicate with the sink node (central node) and this could easily drain the sensor batteries of the CH nodes.

v. *Collaborative lightweight trust-based (CLT) routing protocol* (Mulligan, 2007): This protocol focuses on a collaborative trust effort among nodes while minimizing memory overhead and battery dissipation in nodes. The novelty of this system is the employment of a trust counselor which monitors, warns and improves any node whose trust level is diminishing. It achieves this by utilizing a sliding window system to develop a trust history of all neighbors' nodes. It further uses an aging mechanism to determine misbehaving nodes within the network and thus uses this to prevent various attacks. The paper claims that the protocol could prevent black hole, on-off, bad mouthing and good mouthing attacks. The system however fails to prove the outcomes for autonomous nodes as may be needed in some application areas. It assumes that all nodes have a unique identity.

Table 2
A summary of secure routing protocols for IoT.

Protocol/References	*Techniques*	*Attacks addressed*	*Brief description*	*Weaknesses*
Secure multi-hop routing for IoT communication(Chze and Leong, 2014)	Multi-layer parameter authentication	Gray hole, black hole sinkhole and spoofing attacks	System authenticates IoT devices before they could join or create a new network. It also uses a multi-layer parameter into the routing algorithm and hence, when nodes want to join the network, they have to authenticate.	Excessive overhead in creating a multi-layer parameter that will host IoT nodes in the network making the protocol unsuitable large scale deployment.
TSRF: A trust-Aware secure routing framework in wireless sensor networks (Hummen et al., 2013)	Direct and indirect trust metric system	On-off attack, conflicting behavior attack, selfish attack, bad mouthing attack and collusion attack.	A system designed for WSNs and based on trust derivation which is a direct and an indirect observations of behavioral patterns of sensor nodes with trust values among nodes represented in a range from 0 (no trust) to 1 (absolute trust).	The system expended too much memory due largely to the complex trust computations among the nodes. Also, rogue nodes were identified based on previous trust history which implies that new rogue nodes behaving well for a while will evade detection.
Two-way acknowledgment-based trust (2-ACKT) (Anita et al., 2013)	Direct trust metric between nodes	Blackhole, spoofing and selfish behavior attacks	The scheme is based on a dual acknowledgment system in developing trust among neighboring nodes while creating a route to the sink node with a third party sponsor that creates the two hop acknowledgment in the network.	Does not detect greyhole attacks and the trust relationships is not in consonance with the state of the network since neighboring nodes are not the source of the recommendations.
The group-based trust management scheme (GTMS) (Krentz et al., 2013)	Trust computation using direct observation of nodes	Addressed black hole attacks	A trust management scheme involving the computation of trust using the number of successful and unsuccessful interactions among nodes and indirect observations among nodes while using Cluster Heads (CH) at intragroup level for gathering recommendations from all its group members.	The cluster heads at the intragroup level had a high energy requirement for them to communicate with the sink node and this drains the sensor batteries of the cluster head nodes.
Collaborative lightweight trust-based (CLT) routing protocol (Mulligan, 2007)	Collaborative trust effort among nodes	black hole, on-off, bad mouthing and good-mouthing attacks	Protocol which uses a trust counselor in monitoring and warning nodes with diminishing trust levels through the use of a sliding window system to develop a trust history of all neighbors' nodes. It also employs an aging mechanism to determine misbehaving nodes within the network and thus prevent network attacks.	The system fails to prove the outcome for autonomous nodes as may be needed in some application areas and assumes that all nodes have unique identity.
Lithe: Lightweight Secure CoAP for the Internet of Things (Raza et al., 2013)	DTLS compression Mechanisms for CoAP	Fragmentation attacks, end-to-end secure delivery of data in CoAP.	A 6LoWPAN datagram transport layer security (DTLS) compression protocol for CoAPs which extended the 6LoWPAN standard and introduced an integration module for header compression and end-end delivery of data packets in CoAP.	System involves use of cryptographic processing of record and handshake protocols which are computationally expensive and the system is still susceptible to attacks like gray hole, black hole sinkhole and spoofing attacks
Security access protocols in IoT networks with heterogeneous non-IP Terminals (Giuliano et al., Vegni, 2014)	Time-based key-generating server system	Prevents replay attacks	A time-based system which generates keys for secure transaction between short range non-IP devices. A security procedure is used for both uni- and bi-directional devices, contingent on the devices' capabilities. The security algorithms are based on a local key renewal while considering the local clock time.	A potential weakness is with the mediator server being compromised. De-synchronization, replay and reader impersonation attacks will be very possible. Also the system assumes IoT devices have GPS system which is rarely the case.
Secure communication for the Internet of Things— a comparison of link-layer security and IPsec for 6LoWPAN (Raza et al., 2014)	IPsec	Secure end to end transmission	This system explores the use IPsec as a security mechanism for secure end-to-end transmission in IoT. An IPsec extension was designed based on 6LoWPAN through the extension various header in the 6LoWPAN frame header format while also taking advantage of the cryptographic system within the IEEE 802.15.4 transceivers for 6LoWPAN/IPsec.	A complex protocol design as protocol does not accomplish a trade-off between simplicity and compatibility – The approach seeks to apply IPsec to resource constrained devices by harmonizing link-layer security and IPsec security
Energy-efficient probabilistic routing algorithm for Internet of Things (Sang-Hyun et al., 2014)	Node residual energy and expected transmission (ETX) count	None.	A protocol which controls the broadcast of the routing request packets stochastically so as to boost network lifetime while reducing packet loss due to flooding. Using the residual energy of a node and the expected transmission (ETX) count as the routing metrics, the system stochastically controls the	Susceptible to all forms of attacks.

			number of route requests hence gaining an improved energy-efficient route setup.	
An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications (Duan et al., 2014)	Trust Derivation Dilemma Game system	Bad mouthing, DoS and Selfish attacks	A game theoretic energy-aware secure protocol for IoT which proposes a risk approach model in finding the best number of recommendations which fuls the network security requirements. The trust derivation dilemma game (TDDG) is introduced into the trust derivation system based on the optimal recommendations received while the mixed strategy Nash equilibrium is used to compute the probability of the selected strategy.	Excessive overhead produced by trust request which degrades the performance of the network. The network is also susceptible to attacks such as greyhole, black hole.
A standard compliant security framework for IEEE 802.15.4 networks (Piro et al., 2014)	Encryption and authentication.	Replay attack	A security compliant framework developed for setting up and managing secure IEEE 802.15.4 networks. The framework envisions some likely secure configurations in a low-power and lossy network while describing how each could be used in defending against layer 2 attacks (MAC) through a key exchange.	The framework does not extend to the layer 3 (routing layer) which makes it vulnerable to layer 3 attacks such spoofing, bad mouthing, greyhole and black hole attacks.
6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach (Le et al., 2012)	Statistical-based intrusion detection system (IDS) and Cryptography	Gray hole, Black hole Sinkhole, spoofing attacks, selfish attack, bad mouthing attack and collusion attacks.	A 6LoWPAN IDS framework for securing network operations at the link layer. The paper proposes the use of an RPL system based IDS for fortifying network topology while utilizing a statistical anomaly method in guaranteeing performance of nodes.	A framework yet to be implemented and tested.
Optimal and secure protocols in the IETF 6TiSCH communication stack (Accettura and Piro, 2014)	6TiSCH	Addressing security issues at the MAC layer as found in 6LoWPAN and RPL.	Presents a work-in-progress of the standardization effort of the new routing protocol which hopes to address the optimal distributed scheduling technique that is able to assign resources between network nodes in an efficient manner and providing a scalable system which supports the setting up and management of secured domains for the industrial sector.	This is yet to be seen as 6TiSCH is still a work-in-progress.

Table 3
A comparative study of secure routing protocols for IoT.

Protocol/References	*Complexity (high/medium/low)*	*Scalability*	*Protocol evaluation*
Secure multi-hop routing for IoT communication (Chze and Leong, 2014)	Low	Scales well with a few nodes but does not scale on large number nodes.	Protocol tested on a live testbed. Physical deployment of devices.
TSRF: A trust-aware secure routing framework in wireless sensor networks (Hummen et al., 2013)	High	Not scalable as the system expends significant amount of memory due largely to the complex trust computations among the nodes.	System tested using simulator (NS-2)
Two-way acknowledgment-based trust (2-ACKT) (Anita et al., 2013)	Medium	Not Available	System tested using simulator (NS-2)
The group-based trust management scheme (GTMS) (Krentz et al., 2013)	High	Scales well for up to 10,000 sensor nodes however, consumes much memory and depletes battery of cluster heads during communication with sink node.	Mathematical proof and simulation based evaluation (Sensor Network Simulator and Emulator (SENSE))
Collaborative lightweight trust-based (CLT) routing protocol (Mulligan, 2007)	Medium	Not available.	Mathematical proof and simulation based evaluation (NS-2)
Lithe: Lightweight secure CoAP for the Internet of Things (Raza et al., 2013)	High	Not scalable as system involves use of cryptographic processing of Record and handshake protocols which are computationally expensive.	System tested using simulation (Contiki/Cooja)
Security access protocols in IoT networks with Heterogeneous non-IP Terminals (Giuliano et al., Vegni)	Low	Scalable for non-IP based IoT devices.	System tested using simulation
Secure communication for the Internet of Things— a comparison of link-layer security and IPsec for 6LoWPAN (Raza et al., 2014)	High	Not scalable as protocol does not accomplish a trade-off between simplicity and compatibility.	System tested using simulation (Contiki/Cooja)
Energy-efficient probabilistic routing algorithm for Internet of Things (Sang-Hyun et al., 2014)	Low	Not available.	System tested using simulator (NS-2)
An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications (Duan et al., 2014)	Medium	Not available	System tested using simulator (NS-2)
A standard compliant security framework for IEEE 802.15.4 networks (Piro et al., 2014)	Medium	Not available	A conceptual framework
6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach (Le et al., 2012)	Low	Not available	A logical concept
Optimal and secure protocols in the IETF 6TiSCH communication stack (Accettura and Piro, 2014)	High	Not available (work in progress)	A proposed standard

5. Trust in IoT secure routing

Trust can be defined as the affiliation between two parties, where one party (trustor) is ready to count on the (expected) actions performed by the second party (trustee). In other words, the trustor is the evaluator while the trustee is been evaluated to determine its trust level. The authors in Gambetta (1988) have defined trust as the certain subjective possibility where an agent (node) examines a fellow agent (node) or group of agents (nodes) and believing they will perform a particular action as expected before it has the opportunity to observe the action within the context as it affects its own action.

Trust can be classified under three categories: *general, situational* and *basic trust. General trust* is the trust an agent or a node has in another without any bias to any particular condition. *Situational trust* is the trust an agent or a node has in another due to a peculiar experience or situation. *Basic trust* is based on the past experiences a node has in general towards another node. In the field of communications and networking, the concept of trust is an attractive topic as trust could be embedded in communication and network protocol designs. Cooperation and collaboration are considered critical in the development of trust relationships among participating nodes as these determine the scalability, survivability, dependability and secure operations of the network. Trust among nodes is founded on the basis that, trusted nodes will not perform maliciously under given circumstances.

Trust modeling is a useful practice of estimating the level of reliability among devices within a system. It pinpoints the concerns which could affect the trust of a system while helping to identify areas where a low value of trust could degrade a system's operational efficiency and usability. The study of trust among IoT sensor nodes is particularly attractive, since it is lightweight and hence, suites resource-constrained IoT nodes.

Researchers have proposed different types of trust models for secure routing in sensor networks, like, Bayesian, Game theory, Entropy, Fuzzy, Probability, Neural network, Swarm intelligence, Directed/undirected graph, Arithmetic/weighting and Markov chain, which have their own pros and cons. These models can be considered for IoT routing as well. Table 4 provides a summary of these models.

6. Secure routing in IoT: issues and challenges

The lack of standardization in secure routing among IoT devices raises a lot of concerns related to the current security level of routing practiced in IoT networks. While the security consequences for IoT remains imminent and near perhaps, the introduction of a secure routing framework could as well become the foundation to the execution of security in the IoT system. Today, the growth of IP-based sensors implies a further increase of possible attacks in IoT. This highlights the need for new or improved security protocols and identification techniques in IoT. It is without any doubt that IoT presents fresh challenges to network and security designers. IoT enabled devices which communicate with one another, identify threats and anomalies will need to evolve to cope with this fresh challenges. We explore further IETF standard routing protocols while pointing possible research challenges.

6.1. 6LoWPAN: research challenges

The IETF RFC 4944 (Montenegro et al., 2007; Pister et al., 2009) although identified the idea of adopting various security

Table 4
A Summary of trust models for secure routing in sensor networks.

Trust models	Description
Bayesian trust model	This model utilizes the Bayes theorem in arriving at the truth of a value using probability distributions. It expresses how a subjective degree of trust should realistically change to be considered as evidence (Dubey, Tokekar; Gao and Liu, 2014; Melaye and Demazeau, 2005).
Game theory trust model	This model relies on strategic decision making which normally involves two or more players in order to reach an optimal solution. Through this the best trust value can be obtained in making a decision (Feng et al., 2014; Yuanjie et al., 2015).
Entropy trust model	This takes into account the data communicated among the nodes and based on probabilistic distribution, it considers the set of all trust values of all the nodes and computes their values using probability distributions. From those values it considers the one with the highest information entropy (trust) and this value is used as the trust for making a decision of the best route to follow (Che et al., 2015; Sovan and Arnab, 2013).
Fuzzy trust model	This model relies on a form of multi-valued logic which involves giving varying levels of values to a certain truth because of their variableness. This is used in comparison with the traditional binary logic where variables (trust) could assume either true or false (0 or 1) and not a variation of values (Raje, Sakhare; JØSANG, 2001).
Probability trust model	It focuses on the probability distribution of values (trust) in even (normal) manner using the analysis of random phenomena. The essential entities of probability theory are random variables, and events (observable behavior of nodes) (Xu et al., Shi; Yuan, 2011).
Neural network model	This model uses artificial intelligence to determine the behavior of nodes in a sensor network. It seeks to simulate the behavior of a rational person while being applied to sensor nodes (Po-Jen and Yi-Jun, 2014; Singh and Agrawal, 2013).
Swarm intelligence model	A model based on the communal behavior of distributed, self-organized systems. This system employs a collection of agents (nodes) relating locally with each other within their neighborhood. The idea is from the biological ecosystem of living things within their environment. Although there is no specific way the nodes are expected to behave, with the random interaction among the agents a common trust behavior is developed and adopted (Gupta et al., 2014; Wei and Di, 2014).
Directed and undirected graph model	A model derived from graph theory in mathematics that represents nodes as a set of vertices and the communication links as a set of edges connecting the vertices. Through some mathematical computation the nodes are assigned values regarded as the trust levels between each nodes while the direction of the links determine the direction of communication between the nodes (Yanhua and Zhi-Li, 2013; Kowshik and Kumar, 2012).
Arithmetic/Weighting trust model	This model considers product of trust as reputation. The product of past actions and observations are considered as direct reputation and an aggregated weight is assigned in order to determine the trust value of each node and this is used in order to assess the authenticity of any information from a node (Swaruba and Ganesh, 2014; Sai et al., 2010).
Markov chain model	Essentially a key management trust model. This approach evaluates the trust value and distributes trust certificates for key management. Trust values are evaluated based on Markov chain analysis whereby each one-hop neighbour's trust value is examined with respect to their past trust performance. The trust value is estimated and sent across all nodes. From the trust estimates, the node with the highest trust value is selected as the key management certification authority (Vasim babu and Ramprasad, 2012; Xiaolong and Donglei, 2014).

mechanisms within the concept of the 6LoWPAN adaptation layer, it however, addressed only the general security threats and requirements, and there is still no security implementation. We present below a number of proposed solutions to the open research challenges in guaranteeing the IoT network-layer for a secure route communications using 6LoWPAN.

The Internet Protocol Security (IPSec) (Kent, 2005a, 2005b; Seo and Kent, 2005) design facilitates the authentication and encryption of IP packets operating at the network layer during a communication session. It further provides support for Virtual Private Networks (VPN) while in different operation modes. As indicated earlier, end-to-end network-layer security may find their usefulness in future IoT deployments and these IoT devices will be required to be in sync with other internet devices that are more resource endowed than them. Notwithstanding the benefits of end-to-end network layer security and the proposal in the RFC 4944 of the IETF standard, no precise security model have been defined for adoption regarding the 6LoWPAN adaptation layer.

A major challenge to the adoption of IPSec and IKE in 6LoWPAN as a network layer security is predicated on the resource constraints of the sensing nodes and a comprehensive study to buttress this have been presented by Riaz et al. (2009) and Shelby and Bormann (2011). Furthermore, a look at other means of securing network routes like frame header compression and embedding the concept of efficient trust models to work in consonance with the 6LoWPAN adaptation layer will facilitate secure end-to-end communications at the network layer while providing guarantees regarding the confidentiality, integrity, authentication and non-repudiation of network data.

Additionally, some proposals have been put forward which emphasized on the implementation of compressed security headers for the adaptation layer of 6LoWPAN while achieving the same goal as the existing Authentication Header (AH) and Encapsulating Security Payload (ESP) headers of the Internet Protocol Security (IPSec) as proposed in Kent (2005a,2005b) and Seo and Kent (2005). This approach was strengthened by Granjal et al. (2008), where the authors submitted that the introduction of compressed security headers within the adaptation layer was promising so long as a careful design pattern is followed and the various technology platforms could support a seamless hardware security optimization. In another submission, the same authors further advanced and performed a trial evaluation of the usage of AH and ESP compression header security for 6LoWPAN in tunnel and transport modes using AES/CCM encryption at the hardware layer and a presumed application security profile (Granjal et al., 2010, 2014). More recently, Raza et al. (2011) considered the design of header compression security for 6LoWPAN, in this case using a context sharing LOWPAN_IPHC header compression. A detailed review of this proposal and evaluation against IEEE 802.15.4 link layer security has been presented in Raza et al. (2012). A basic advantage of the header compression proposals is in the usage of the more recent IPHC header compression scheme since it supports the use of IPv6 for global and multicast usage. With the proposals of these research authors presented above for the support of 6LoWPAN network security layer, this will obviously require the support of industry and technology players that will either support the compression security header philosophy or support the end-to-end network security implementation via a security gateway. Both aspects represent opportunities for research, like creating a design of mechanisms to support the conversion between IPSec and 6LoWPAN security, or the mediation of gateways during key management, and key mapping operations. This of course is in addition to decision by industry players as to what is practicable and beneficial in the interest of the industry, sustainability and future development of the technology.

Addressing the security concerns of 6LoWPAN Hummen et al. (2013) substantiated the consequences of packet fragmentation attacks which is a major issue affecting 6LoWPAN. The occurrence of these attacks make buffering, forwarding and handling of fragmented packets challenging for these devices running 6LoWPAN since a malicious node could send spurious, identical or overlapping fragments which could alter the normal network flow. All these occur because of the lack of verification at the 6LoWPAN adaptation layer, since the receiving nodes have no way of differentiating fake fragments from the authentic frames during fragment reassembly. The consequences of fragmentation attacks range from getting buffer overflow to the mismanagement of the available computational capability on the sensory devices. The authors suggested the introduction of new field fragmentation headers of 6LoWPAN in order to address the fragmentation attacks like using a timestamp, which protects against unidirectional fragment replays and a one-time protection mechanism against bidirectional fragment replays.

Also, Hummen et al. (2013) proposed the use of an authentication mechanism which performs a per-fragment sender authentication and removal of messages from the receiver's buffer, for nodes considered suspicious. The authors employed a hash chain system, which grants a legitimate sender the authority to add an authentication value to each fragment during the 6LoWPAN fragmentation. In the event of an overflow the receiver has the option of deciding which fragments to discard. This decision is based on the quantum of frames captured and processed and the sending behavior of the source node. Although this scheme does not necessitate any adjustments to 6LoWPAN frame formats, it is rather obvious that the proposed security mechanisms will have to be co-opted into the adaptation-layer of 6LoWPAN.

In the formal specification of 6LowPAN standard, key management was a vital security functionality considered in the 6LoWPAN. This aspect could be considered a cross layer security that is interconnected with authentication since keys need to be negotiated and intermittently refreshed to guarantee effective and lasting security regardless of the layer at which the communication may ensue. Although the authors did not put forward any definite key management solution, however, RFC 6568 (Kim and Kaspar, 2012) shows the likelihood of adopting a simple but effective Internet key management solutions. For example, minimal IKEv2 (Hummen et al., 2013) co-opts Internet key management to resource-constrained sensing in environmental locations while preserving its compatibility with the current Internet standard. In Roman et al. (2011), the authors proposed that public-key management strategies could necessitate the use of nodes which are more powerful than the state-of-the-art sensing platforms, especially if they require supporting services. Other proposed methods which could be explored include the introduction of a new lightweight key management technique suitable for the specific IoT device environment.

6.2. RPL: research challenges

Although the IETF RPL standard includes versions which attempt to secure route control messages using simple security procedures, it however suffers from having a basic system for supporting important secure routing operations. We present below a discourse on the current state of research in RPL while focusing on the security of RPL.

In our study, we note that even though the secure versions of RPL which attempt to secure the route control messages, there are no extra security mechanisms implemented in the present version of RPL protocol standard (Winter et al., 2012). We investigated and found that RPL suffers from the following attacks, falsification attacks, routing information replay, byzantine attacks, physical device compromise or remote device access attacks, selective-forwarding attacks, sinkhole attacks, black hole attacks and gray hole attacks, version number manipulation attacks (Wallgren et al., 2013; Tsao et al., 2014; Mayzaud et al., 2014). The RPL IETF ROLL report further discussed the general security requirements and goals, but did not give specific security models for RPL. It would be worthwhile investigating into the various security threat models specific to RPL and to its application areas and to eventually develop systems to protect RPL routing protocol from threats identified.

Furthermore, the present RPL standard (Winter et al., 2012) mainly addresses the management of keys with applications using device pre-configuration and how such devices could join a network using a preconfigured common group key or a key learned from a trusted DIS configuration message. It does not describe how authentication and secure network connection mechanisms could be designed to facilitate other devices which are dynamic and run security critical applications. A research possibility for routing profiles in RPL could be the definition of routing profile for specific application areas. A further investigation and standardization could be to survey the design of security policies describing how security could be used in protecting routing operations with reference to an application area. The policies could further establish the requirements of applications with reference to confidentiality, integrity, authenticity, non-repudiation and the ability to replay control messages within the network.

The authors in Tsao et al. (2014) have presented open issues with respect to the security of RPL. They presented various threat analysis against ROLL routing systems while making contributions on how to address these threat challenges. The authors in their study, identified threats by using the ISO 7498-2 security reference model as specified in Parker (1991) which listed the various attributes of a good and secure communication and these include access control, authentication, confidentiality, integrity and non-repudiation, and availability. The model defines what to protect while also identifying possible vulnerable points needing protection that could be undermined in the network. The model supports the classification of the threats and the precise attacks relating to confidentiality, integrity and availability of routing and control message exchanges in the perspective of routing protocols in ROLL. The paper further advanced a security framework for ROLL protocols which is based on earlier work on security for routing while adjusting the parameters to suit the constraints peculiar to the 6LoWPAN environments. Within this framework, security features are enumerated which could be adapted and fitted within the RPL perspective along with some general system security features which could affect the routing protocol however, this requires serious attention as the method to be adopted and the impact goes beyond the routing protocol itself. The evaluation presented in this study could give a promising pathway to good security recommendations for integration into the ROLL protocols. It is noteworthy that the implications of the various security recommendations presented for the ROLL protocols presents possible issues for future research consideration.

A look at the aspect of RPL security, as presently proposed in Winter et al. (2012) provides security only against external attacks. An internal attacker who has compromised a node within the network could selectively inject routing messages with malicious purposes. The presenters in Anhtuan et al. (2013) gave a comprehensive analysis of the internal attacks on RPL, with specific attention on the rank property as imbued by RPL protocol. Rank in RPL is used for the prevention of loop, route optimization, and for the minimization of route control overhead. The paper further presented the attacks against the rank property of RPL and the impact on network performance. They identified that the limitation in RPL was largely because a child node does not have

access to the control messages of its parent(s) and hence unable to determine what services its parents are providing thus, for a compromised parent node, a child node will certainly follow the unstable and compromised route. While not putting forward a new scheme for detecting parental activities the paper however, recommended the integration of techniques in RPL that could aid the child node to observe the behavior of its parents in order to defend against internal attacks coming from the parent node.

Dvir et al. (2011) discussed internal attacks and submitted that an internal attacker is capable of undermining a node so as to mimic a gateway (like the DODAG root) or a node within the circumference of a gateway. The authors in their submission proposed the use of a version number with a rank authentication scheme centered on one-way hash chains which links the version numbers with the authentication information (MAC codes) and signatures. This system provides a good defense against internal attackers capable of sending DIO messages using higher version numbers or attackers with capabilities of issuing higher rank values. The purpose of an attacker sending higher version number is to impersonate the DODAG root node and commence the creation of the routing topology, while an attacker issuing higher rank values is to force a larger part of the nodes in the network to connect to the DODAG root via the attacker hence, giving the attacker the leverage of eavesdropping and manipulating a part of the network traffic. The paper gave an evaluation of performance against the impact of these mechanisms on computational time but, did not address the energy impact and memory requirements which are a constraint on these IoT devices.

The authors in Weekly and Pister (2012) focused on various internal attacks against RPL. In their submission, the authors reflected on the impact of sinkhole attacks on RPL networks. They scrutinized the end-to-end data delivery performance in the presence of sinkhole attacks. Sinkhole attacks undermine a node by capturing and dropping its routing and control messages. The authors recommended the blend of a parent fail-over system with a rank authentication scheme. They further illustrated their idea using simulation results to prove that the blend of the two approaches gave promising results and that by populating the network the permeation of sinkholes could be mitigated without requiring to know the specific location of the sink hole nodes within the network. Their rank-authentication system was centred on one-way hash chains provided in Dvir et al. (2011), whereas the parent fail-over scheme uses an end-to-end acknowledgment system which the DODAG root controls.

To recap, various research proposals have been presented in order to address security research challenges in RPL, specifically referencing the threat models and internal attacks to 6LoWPAN and RPL. These proposals could help in evolving and delivering useful contributions for addressing the security loopholes of these protocols and their subsequent adoption as possible standards in the future. A leaf could be taken from the other similar areas to IoT routing such as the wireless sensor networks (WSNs), mobile ad hoc networks (MANETs) where extensive research knowledge has been built over time and various approaches have been proposed. This may guide in the final adoption of a truly secure routing framework for IoT devices so long as with proper internalization and the efficient and proficient design to fit the requirements of IoT routing protocols.

Finally, while not restricting the study to key management only, other secure routing techniques such as the concept of trust systems which have also been researched and applied in WSNs and MANETs and have even found practical application in various computing fields could also be explored with the intent of adapting them to fit with the secure routing needs of IoT protocols.

6.3. Designing and developing secure IoT routing protocols: recommendations

With the number of IoT networks on the rise worldwide, the need for secure routing protocols is becoming salient. To design and develop a secure protocol, it is important to identify and address the security goals of the protocol while complying with defined security and privacy standards. Moreover, the security objectives must not inhibit the basic information requirements of a data network, which are confidentiality, integrity and availability. We outline below few secure IoT routing protocol design recommendations for the research community to consider:

i. *Secure route establishment:* An important feature of any secure routing protocol is its ability to establish and guarantee a secure route between source and destination while isolating malicious nodes in the network (Abdelaziz et al., 2013).
ii. *Self-stabilization:* The self-stabilization feature of a good secure routing protocol implies that the protocol must be able to recover automatically from any problem within a certain time without human intervention. An attacker who transmits spurious packets to destabilize the network may initially make the network unstable but through the enabled self-stabilization feature, the network should be able to recover over time (and function normally) and isolate the malicious node(s) (Airehrour and Gutierrez, 2015).
iii. *Effective malicious node identification system:* A malicious node isolation mechanism maybe effectively embedded in the protocol design to isolate misbehaving nodes within the network. The misbehaving nodes must have minimal effect in tampering/disrupting the network routing process.
iv. *Lightweight computations:* IoT nodes are generally resource constrained and have limited computational capabilities and memory. Any secure routing protocol design thus should ideally consider lightweight but secure metric system. Secure routing operations such as public key cryptography or shortest path algorithms should ideally be limited to only few nodes to reduce complexity. It is advisable to perform encryption only at the route endpoints during route creation. This will help defend against the denial-of-service attacks common to sensor networks (Airehrour and Gutierrez, 2015).
v. *Location privacy:* Maintaining the location privacy of the IoT nodes in a network is a crucial security requirement. While designing and developing a secure routing protocol, it needs to be taken into account that the protocol is capable enough to prevent the extraction of location specific information of IoT nodes and the network topology. This is, however, a limitation with multi-hop routing topology with a fixed set of root (sink) nodes because once few nodes surrounding the sink nodes are compromised, the network likely becomes vulnerable. Having an arbitrarily revolving set of virtual cluster head nodes which creates an overlay network may prove to be helpful in such situations. A multi-hop topology is constructed using the selected virtual cluster head nodes and the cluster heads then communicate directly with the authentic root node. The set of virtual cluster head nodes, however, needs to frequently change to make it difficult for the malicious nodes to identify the appropriate nodes to compromise.

Having protected secure routing is of utmost importance in IoT networks for the different applications to run safely. Our survey, however, has shown that current protocol standards for these networks are insecure, specifically because most IoT networks are self-organizing and operate without human intervention and thus, malicious nodes could very well be introduced into the network in order to compromise the nodes.

7. Conclusions

In IoT networks, secure routing plays an essential role in the seamless and safe functioning of the entire network. As noted in Karlsson et al. (2012) and Hakak et al. (2014) finding a universal solution applicable to all the routing attacks (present and future attacks) in IoT nodes is an intractable problem. This is because most malicious attacks have individual mode of operation and pre-empting future types of attacks may prove rather difficult. However, having a solution that can effectively address a number of these routing attacks may prove to be a novel accomplishment. In this survey, we carried out an in-depth research study and analysis of the secure routing protocols in IoT networks. The different systems currently being used for secure routing communications among the IoT nodes are studied. The survey also highlights that traditional IoT routing protocols (6LowPAN and RPL) lack appropriate security implementations and discusses in detail the existing literatures elucidating their proposals, the limitations and potentials for future extensions. Different security techniques, like, key management, cryptography and trust management are explored as well. Moreover, the study showed that IoT nodes need reduced energy consumption with lower cost requirements. Based on our discussions in the work, a list of recommendations for the future design and developing of secure routing protocols is provided. In a nutshell, the recommendations stated that protocol designers, while adhering to security and privacy standards of a secure routing protocol, must minimize the security impact on the network in order to deliver an acceptable network performance of a data network. As further extension of this work, we plan to design and develop secure trust-based IoT routing protocols that will help to deal with common malicious attacks in IoT networks.

References

Abdelaziz, A.K., Nafaa, M., Salim, G., 2013. Survey of routing attacks and countermeasures. In: Proceedings of the 15th International Conference on Computer Modelling and Simulation (UKSim). 693–698.

Accettura N, Piro G. Optimal and secure protocols in the IETF 6TiSCH communication stack. Ind. Electron. (ISIE) IEEE 23rd Int. Symp. 2014:1469–74.

Airehrour D, Gutierrez J. An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing. Ontario, Canada. CONF-IRM 2015 2015.

Amin SO, Siddiqui MS, Hong CS, Choe J. A novel coding scheme to implement signature based IDS in IP based Sensor Networks. Integr Netw Manag-Work, 2009 IM'09 IFIP/IEEE Int Symp 2009:269–74.

Anderson, R., Kuhn, M., 1996. Tamper resistance: a cautionary note Oakland, California. Present Proceedings of the 2nd Conf Proc Second USENIX Workshop Electron Commer, 2.

Anhtuan L, Loo J, Lasebae A, Vinel A, Yue C, Chai M. The impact of rank attack on network topology of routing protocol for low-power and lossy networks. Sens. J. IEEE 2013;13:3685–92.

Anita X, Manickam J Martin Leo, Bhagyaveni MA. Two-way acknowledgment-based trust framework for wireless sensor networks. Int J. Distrib. Sens. Netw. 2013;2013:14.

Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput. Netw. 2010;54:2787–805.

Awerbuch B, Holmer D, Nita-Rotaru C, Rubens H. An on-demand secure routing protocol resilient to Byzantine failures. Proc. ACM Workshop Wirel. Secur. 2002:21–30.

Becher A, Benenson Z, Dornseif M. Tampering with motes: real-world physical attacks on wireless sensor networks. York, UK. Present Proc Third Int Conf Secur Pervasive Comput 2006.

Che S, Feng R, Liang X, Wang X. A lightweight trust management based on Bayesian and Entropy for wireless sensor networks. Secur Commun Netw 2015;vol. 8:168–75.

Cheng M, Xuan G, Lin C. Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks. IEEE Trans. Wirel. Commun. 2009;8:3770–9.

Chugh K, Aboubaker L, Loo J. Case Study of a Black Hole Attack on LoWPAN-RPL. Rome, Italy (August 2012). Proc Sixth Int Conf Emerg Secur Inf, Syst Technol (SECURWARE) 2012:157–62.

Chze PLR, Leong KS. A Secure Multi-Hop Routing for IoT Communication. IEEE World Forum Internet Things (WF-IoT) 2014:428–32.

CISCO. (2013, December 2, 2014). The Internet of Everything (IoE): Connections Counter. Available: ⟨http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342⟩.

CTIA-The Wireless Association. (2014, December 2, 2014). Mobile Cybersecurity and the Internet of Things Empowering M2M Communication. [White paper]. Available: ⟨http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf⟩.

D. Evans. (2011, 29 November, 2014). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Available: ⟨http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf⟩.

Duan J, Gao D, Yang D, Foh CH, Chen H-H. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. IEEE Internet Things J. 2014;1:58–69.

Dvir A, Holczer T, Buttyan L. VeRA-version number and rank authentication in rpl. Mob. Adhoc Sens. Syst. (MASS), 2011 IEEE 8th Int. Conf. 2011:709–14.

Ericsson. (2011, December 2, 2014). More than 50 billion connected devices: Driving forces. Available: ⟨http://www.akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf⟩.

European Union, 2014. Opinion 8/2014 on the on Recent Developments on the Internet of Things.

Feng R, Che S, Wang X, Wan J. An incentive mechanism based on game theory for trust management. Secur Commun Netw 2014;vol. 7:2318–25.

Gagandeep, Aashima. Study on sinkhole attacks in wireless Ad hoc networks. Int J. Comput. Sci. Eng. (IJCSE) 2012;4:1078–84.

Gambetta D. Can we trust trust? Oxford, England, UK: Basil Blackwell; 1988.

Gao Y, Liu W. BeTrust: a dynamic trust model based on bayesian inference and tsallis entropy for medical sensor networks. J. Sens. 2014;2014:1–10.

García-Teodoro P, Sánchez-Casado L, Maciá-Fernández G. Taxonomy and Holistic Detection of Security Attacks in MANETs. In: Khan S, Lloret Mauri J, editors. Security for multihop wireless networks. Boca Raton, FL: Auerbach Publications; 2014. p. 3–11.

Gartner. Gartner Says 4 9 Billion Connect "Things" Will Be Use 2015 2014.

Granjal J, Monteiro E, Silva JS. Enabling network-layer security on IPv6 wireless sensor networks. Glob Telecommun Conf (GLOBECOM 2010), 2010 IEEE 2010:1–6.

Granjal J, Monteiro E, Silva JS. Network-layer security for the Internet of Things using TinyOS and BLIP. Int Journal Commun Syst 2014;vol. 27:1938–63.

Granjal J, Silva R, Monteiro E, Sa Silva J, Boavida F. Why is IPSec a viable option for wireless sensor networks. Mob Ad Hoc Sens Syst, 2008 MASS 2008 5th IEEE Int Conf 2008:802–7.

Gu Y, Ji Y, Li J, Zhao B. ESWC: efficient scheduling for the mobile sink in wireless sensor networks with delay constraint. IEEE Trans Parallel Distrib Syst 2013;24:1310–20.

Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 2013;29:1645–60.

Gupta A, Pandey OJ, Shukla M, Dadhich A, Ingle A, Gawande P. Towards context-aware smart mechatronics networks: integrating swarm intelligence and ambient intelligence. Issues Challenges Intell Comput Tech (ICICT), 2014 Int Conf 2014:64–9.

Hakak S, Abd Latif S, Gilkar G, Alam MK. Performance analysis of DYMO and DSR protocols under variation of DSSS rate. Inform. Electron Vision (ICIEV), 2014 Int. Conf. 2014:1–6.

Hamid A, Mamun Or R, Seon H Choong. Defense against lap-top class attacker in wireless sensor network. Adv. Commun. Technol. 2006 ICACT 2006 8th Int. Conf. 2006;318:5.

Hennebert C, Dos Santos J. Security protocols and privacy issues into 6LoWPAN stack: a synthesis. Internet Things J. IEEE 2014;1:384–98.

Hu Y, Perrig A, Johnson D. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. ACM Workshop Wirel Secur (WiSe) 2003:30–40.

Hui J, Thubert P. Compression format IPv6 datagrams IEEE 802 15 4-based Netw 2011.

Hummen R, Wirtz H, Ziegeldorf JH, Hiller J, Wehrle K. Tailoring end-to-end IP security protocols to the Internet of Things. Netw Protoc (ICNP), 2013 21st IEEE Int Conf 2013:1–10.

Internet Engineering Task Force (IETF). (December, 2014, December 1, 2014). IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch). Available: ⟨https://datatracker.ietf.org/wg/6tisch/charter/⟩.

Ishaq I, Carels D, Teklemariam G, Hoebeke J, Abeele F, Poorter E, et al. IETF Standardization in the Field of the Internet of Things (IoT): A Survey. J. Sens. Actuator Netw. 2013;2:235–87.

Islam N, Shaikh ZA. Security Issues in Mobile Ad Hoc Network. ed. In: Khan S, Pathan A-SK, editors. Wireless Networks and Security: Issues, Challenges and Research Trends. Heidelberg, Germany: Springer-Verlag Berlin Heidelberg; 2013. p. 49–56.

Dubey, J., Tokekar, V., Bayesian network based trust model with time window for Pure P2P computing systems, pp. 219–223.

JØSANG A. A logic for uncertain probabilities. Int. J. Uncertain, Fuzziness Knowl-Based Syst 2001;09:279–311.

Karlsson J, Dooley LS, Pulkkis G. Routing security in mobile ad-hoc networks. Issues Informing Sci. Inf. Technol. 2012;9:369.

Kasinathan P, Pastrone C, Spirito M, Vinkovits M. Denial-of-Service detection in 6LoWPAN based Internet of Things. IEEE 9th Int. Conf. Wirel Mob Comput, Netw Commun (WiMob) 2013:600–7.

Kent, S., 2005a. IP authentication header.

Kent, S., 2005b. IP encapsulating Secur payload (ESP).
Kim, E., Kaspar, D., 2012. Design Appl spaces IPv6 Low-power Wirel Personal area Netw (6LoWPANs).
Kowshik H, Kumar PR. Optimal function computation in directed and undirected graphs. IEEE Trans. Inf. Theory 2012;58:3407–18.
Krentz, K.-F., Rafiee, H., Meinel, C., 2013. 6LoWPAN security: adding compromise resilience to the 802.15.4 security sublayer Zurich, Switzerland. Present Proc Int Workshop Adapt Secur.
Le A, Loo J, Lasebae A, Aiash M, Luo Y. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. Int. J. Commun. Syst. 2012;25:1189–212.
Liu H, Chu X, Leung Y-W, Du R. Minimum-cost sensor placement for required lifetime in wireless sensor-target surveillance networks. IEEE Trans. Parallel. Distrib. Syst. 2013;24:1783–96.
Machado K, Rosário D, Cerqueira E, Loureiro AAF, Neto A, Souza JN d. A routing protocol based on energy and link quality for Internet of Things applications. Sensors, 13. Switzerland: Basel; 1942–64.
Mayzaud A, Sehgal A, Badonnel R, Chrisment I, Schönwälder J. A Study of RPL DODAG Version Attacks. In: Sperotto A, Doyen G, Latré S, Charalambides M, Stiller B, editors. Monitoring and Securing Virtualized Networks and Services, vol. 8508. Springer Berlin Heidelberg; 2014. p. 92–104.
Mc Afee Labs. (2014, September 13, 2014). 2013 Threats Predictions. Available: ⟨http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf⟩.
Melaye D, Demazeau Y. Bayesian Dynamic Trust Model . Berlin: Heidelberg: Springer Berlin Heidelberg; 480–9.
Miller MJ, Vaidya NH. A MAC protocol to reduce sensor network energy consumption using a wakeup radio. IEEE Trans Mob Comput 2005;4:228–42.
Mishra A. Security and quality of service in Ad Hoc wireless networks. Cambridge, UK: Cambridge University Press; 2008.
Montenegro G, Kushalnagar N, Hui J, Culler D. 2070-1721. Transmission IPv6 Pack IEEE 802 15 4 Netw 2007.
Mulligan G. The 6LoWPAN architecture. Cork, Ireland. Present Proc 4th workshop Embed networked sensors 2007.
Pister, K., Thubert, P., Phinney, T., (2009), Industrial Routing Requirements in Low-Power and Lossy Networks. IETF RFC 5673. Available: ⟨https://tools.ietf.org/html/rfc5673⟩.
Packard Hewlett. Internet Things Res Study (2014 Report) 2015.
Parker DB. Restating the foundation of information security. Comput Audit Update 1991;1991:2–15.
Perrey H, Landsmann M, Ugus O, Schmidt TC, Wählisch M. TRAIL: Topology Authentication in RPL. arXiv Prepr arXiv:1108.0883v1 [gr-qc] 2013;1312:0984.
Pervaiz MO, Cardei M, Wu J. Routing Security in Ad Hoc Wireless Networks. ed. Florida Atlantic University. In: Huang S, MacCallum D, Du DZ, editors. Boca Raton, FL: Springer; 2005.
Piro G, Boggia G, Grieco LA. A standard compliant security framework for IEEE 802.15.4 networks. Internet Things (WF-IoT), 2014 IEEE World Forum 2014:27–30.
Po-Jen C, Yi-Jun J. Effective neural network-based node localisation scheme for wireless sensor networks. Wirel. Sens. Syst. IET 2014;4:97–103.
R. Giuliano, F. Mazzenga, A. Neri, and A.M. Vegni, Security Access Protocols in IoT Networks with Heterogenous Non-IP Terminals, pp. 257–262.
Raje, R.A., Sakhare, A.V., Routing in Wireless Sensor Network Using Fuzzy Based Trust Model, pp. 529–532.
Raza S, Duquennoy S, Höglund J, Roedig U, Voigt T. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. Secur. Commun Netw. 2012.
Raza S, Duquennoy S, Höglund J, Roedig U, Voigt T. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. Secur. Commun Netw. 2014;7:2654–68.
Raza S, Duquennoy S, Chung T, Yazar D, Voigt T, Roedig U. Securing communication in 6LoWPAN with compressed IPsec. Distrib. Comput. Sens. Syst. Work (DCOSS) 2011 Int. Conf. 2011:1–8.
Raza S, Shafagh H, Hewage K, Hummen R, Voigt T, Akademin för innovation d o t, et al. Lithe: lightweight Secure CoAP for the Internet of Things. IEEE Sensors Journal 2013;13:3711–20.
Riaz R, Kim K-H, Ahmed HF. Security analysis survey and framework design for ip connected lowpans. Auton Decentralized Syst, 2009 ISADS'09 Int Symp 2009:1–6.
Roman R, Alcaraz C, Lopez J, Sklavos N. Key management systems for sensor networks in the context of the Internet of Things. Comput Electr Eng 2011;37:147–59.
Sai J, Yuan S-f, Ting-huai M, Chang T. Distributed fault detection for wireless sensor based on weighted average. Int. Conf. Netw. Secur. Wirel. Commun. Trust Comput. (NSWCTC) 2010:57–60.
Sang-Hyun P, Seungryong C, Jung-Ryun L. Energy-efficient probabilistic routing algorithm for internet of things. J. Appl Math 2014;2014.
Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. An authenticated routing protocol for secure Ad Hoc Networks. IEEE J. Sel Areas Commun. Wirel Ad hoc Netw. 2005;23:598–610 (special issue).
Shelby, Z., Chakrabarti, S., Nordmark, E., Bormann, C., 2012. Available: ⟨https://tools.ietf.org/html/rfc6775⟩.
Sarkar SK, Basavaraju TG, Puttamadappa C. Ad Hoc mobile wireless networks principles, protocols, and applications. In: Boca Raton FL, editor. Second Edition CRC Press; 2013.
Seo K, Kent S. Security Arch internet Protoc 2005.
Shelby Z, Bormann C. 6LoWPAN: The wireless embedded Internet. John Wiley & Sons; 2011.
Shelby Z, Hartke K, Bormann C, Frank B. Constrained Appl Protoc (CoAP) Draft-ietf-core-coap-04 (Internet Draft) 2011.
Shibo H, Jiming C, Yau DKY, Youxian S. Cross-layer optimization of correlated data gathering in wireless sensor networks. IEEE Trans. Mob. Comput. 2012;11:1678–91.
Singh P, Agrawal S. TDOA Based Node Localization in WSN using neural networks. Int. Conf. Commun. Syst. Netw. Technol. (CSNT) 2013:400–4.
Singh VP, Jain S, Singhai J. Hello flood attack and its countermeasures in wireless sensor networks. Int. J. Comput. Sci. Issues (IJCSI) 2010;7:23–7.
Smith, 2013. Unpatched TRENDnet IP cameras still provide a real-time Peeping Tom paradise (30.10.15) Available: ⟨http://www.networkworld.com/article/2223785/microsoft-subnet/unpatched-trendnet-ip-cameras-still-provide-a-real-time-peeping-tom-paradise.html⟩.
Sophos Limited, 2013. Security Threat Report 2013. 1.13. (13.09.14) Available: ⟨https://www.sophos.com/de-de/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf⟩.
Sophos Limited, 2014. Security Threat Report. 2–22. Available: ⟨http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf⟩.
Sovan B, Arnab G. Entropy Trust based Approach against IP spoofing attacks in network. Int Journal Comput Appl 2013;67.
Spansion. (2014, November 25). ZigBee mesh networks. Available: ⟨http://core.spansion.com/article/contextual-computing-simplifies-iot/#.VG5sfskXJ8E⟩.
Swaruba P, Ganesh VR. Weighted voting based trust management for intrusion tolerance in heterogeneous wireless sensor networks. Int. Conf. Inf. Commun. Embed Syst. (ICICES) 2014:1–7.
Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., Richardson, M., 2014. A Secur Threat Anal Routing Protoc Low-power lossy Netw (RPL).
Vasim babu M, Ramprasad AV. Discrete antithetic Markov Monte Carlo based power mapping localization algorithm for WSN. IEEE Int. Conf. Adv. Commun. Control Comput. Technol. (ICACCCT) 2012:56–62.
Vermesan O, Friess P. Internet of Things-From Research and Innovation to Market Deployment. River Publishers; 2014.
Watteyne, T., Berkeley, U.C., Winter, T., Barthel, D., 2009. Routing Requirements for Urban Low-Power and Lossy Networks. IETF RFC 5548. Available: ⟨https://tools.ietf.org/html/rfc5548⟩.
Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., et al., 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Available: ⟨https://tools.ietf.org/html/rfc6550⟩.
Wallgren L, Raza S, Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. Int. J. Distrib. Sens. Netw. 2013;2013:11.
Weekly K, Pister K. Evaluating sinkhole defense techniques in RPL networks. 20th IEEE Int. Conf. Netw. Protoc. (ICNP) 2012:1–6.
Wei W, Qi Y. Information potential fields navigation in wireless Ad-Hoc sensor networks. Sensors 2011;11:4794.
Wei W, Yang X-L, Shen P-Y, Zhou B. Holes detection in anisotropic sensornets: topological methods. Int. J. Distrib. Sens. Netw. 2012;2012:9.
Wei W, Xu Q, Wang L, Hei XH, Shen P, Shi W, et al. GI/Geom/1 queue based on communication model for mesh networks. Int J. Commun. Syst. 2014;27:3013–29.
Wei Z, Di L. Routing in wireless sensor network using artificial bee colony algorithm. Int. Conf. Wirel. Commun. Sens. Netw. (WCSN) 2014:280–4.
Wu B, Chen J, Wu J, Cardei M. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Xiao Y, Shen XS, Du D-Z, editors. Wireless Network Security. Springer Science; 2007. p. 110–32.
Xu, H., Liu, Y., Qi, S., Shi, Y. A novel trust model based on probability and statistics for Peer to Peer networks, pp. 2047–2050.
Xiaolong L, Donglei F. Markov chain based trust management scheme for wireless sensor networks. J. Netw. 2014;9:3263.
Xu G, Ding Y, Zhao J, Hu L, Fu X. Research on the Internet of Things (IoT). Sens. Transducers 2013;160:463.
Yanhua L, Zhi-Li Z. Random walks and green's function on digraphs: a framework for estimating wireless transmission costs. Netw. IEEE/ACM Trans. 2013;21:135–48.
Yashiro, T., Kobayashi, S., Koshizuka, N., Sakamura, K. An Internet of Things (IoT) architecture for embedded appliances, pp. 314–319.
Yih-Chun H, Adrian P, David BJ. Ariadne: a secure on-demand routing protocol for Ad Hoc networks. Wirel. Netw. 2005;11:21.
Yoo M, Wu F, Qiao C. Recent advances of ICT convergence on wsn applications. Int. J. Distrib. Sens. Netw. 2015;2015:3.
Yuan Q. The Study on Trust Management Model Based on Probability in Distributed E-Commerce System. Berlin, Heidelberg: Springer Berlin Heidelberg; 312–20.
Yuanjie L, Hongyun X, Qiying C, Zichuan L, Shigen S. Evolutionary game-based trust strategy adjustment among nodes in wireless sensor networks. Int. J. Distrib. Sens. Netw. 2015;2015.
Zhang K, Liang X, Lu R, Shen X. Sybil attacks and their defenses in the internet of things. Internet Things J. IEEE 2014;1:372–83.
Zhao, K., Ge, L., 2013. A survey on the internet of things security. In: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS). pp. 663–667.