Journal of Network and Computer Applications 49 (2015) 112–127

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Autonomic schemes for threat mitigation in Internet of Things

Qazi Mamoon Ashraf*, Mohamed Hadi Habaebi

Department of Electrical and Computer Engineering, University Islam Antarabangsa, Jalan Gombak, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 26 June 2014
Received in revised form
17 November 2014
Accepted 23 November 2014
Available online 16 December 2014

Keywords:
Internet of Things
Autonomy
Security
Self-management
Wireless sensor networks
Self-security

ABSTRACT

Internet of Things (IoT) refers to the expansion of Internet technologies to include wireless sensor networks (WSNs) and smart objects by extensive interfacing of exclusively identifiable, distributed communication devices. Due to the close connection with the physical world, it is an important requirement for IoT technology to be self-secure in terms of a standard information security model components. Autonomic security should be considered as a critical priority and careful provisions must be taken in the design of dynamic techniques, architectures and self-sufficient frameworks for future IoT. Over the years, many researchers have proposed threat mitigation approaches for IoT and WSNs. This survey considers specific approaches requiring minimal human intervention and discusses them in relation to self-security. This survey addresses and brings together a broad range of ideas linked together by IoT, autonomy and security. More particularly, this paper looks at threat mitigation approaches in IoT using an autonomic taxonomy and finally sets down future directions.

Contents

* Corresponding author. Tel.: +60 182600034.
E-mail addresses: mamoonq@gmail.com (Q.M. Ashraf), habaebi@iium.edu.my (M.H. Habaebi).

http://dx.doi.org/10.1016/j.jnca.2014.11.011
1084-8045/© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

During the last three decades, tremendous work on the Internet has led to the growth of Internet of Things (IoT) where intelligent interconnections are being created between diverse objects for a globally integrated communication platform (Iera et al., 2010; Zheng et al., 2011). The main vision behind IoT is that embedded devices, also called smart objects, are becoming Internet Protocol (IP) enabled in an attempt to compute, organize and communicate. IoT is setup and maintained economically and energy-efficiently through sensors attached to these objects. A combination of Internet connected embedded devices, smart objects, sensors and supplementary web-based services makes IoT what it is today (Shelby and Bormann, 2011). Furthermore, it is estimated that IoT market adoption will take around 5–10 more years (Gubbi et al., 2013)

It is the need of the hour to secure the communication channels as well as to introduce the supporting security technologies in the IoT devices (O'Neill, 2014). Security represents a critical component for enabling the worldwide adoption of IoT technologies and applications. Some of the recent security research has focused on network based cryptographic mechanisms (Kothmayr et al., 2013; McCusker and O'Connor, 2011), embedded security (Ukil et al., 2011; Babar et al., 2011), distributed approaches for IoT service provisioning (Roman et al., 2013), security solutions for applications (Chen et al., 2011; Liu et al., 2012) as wellas system security frameworks and strategies (Roman et al., 2011; Pan et al., 2011; Zhou and Chao, 2011). A recent study by Ning et al. (2013) identifies the areas in cyber-entity security, and presents security requirements as well as proposes recommendations to meet those requirements. Some security options are currently provided by the existing Internet protocols; nevertheless the device and network limitations prevent their full use. For example, implementation of full IP security (IPsec) suite to protect mobile devices (Arkko et al., 2004), implementation of transport layer security (TLS), as well as the use of firewalls on each end device is rather restricted (Shelby and Bormann, 2011). Furthermore, innovations such as firewall implementations in the lower layers are inefficient as they can be overridden over the wireless channel directly and remote devices can be stolen and compromised.

IoT can be looked at as a highly dynamic and distributed networked system, composed of a large number of smart objects capable of producing and consuming information. There is a vast set of supporting technologies which are necessary to realize the vision of IoT. These include Radio Frequency Identification Devices (RFIDs), sensors, actuators, and similar machine-to-machine (M2M) communication devices. Historically, IoT referred to RFID based technologies where the security solutions have mostly been devised in a vertically integrated ad hoc manner (Miorandi et al., 2012). Such heterogeneity in technology required specific security mechanisms to meet the requirements. For the wide variety of IoT devices today, there exists a huge tradeoff among performance, cost and security which make security for IoT a big challenge. Consequently, IoT offers a wealth of areas where the security aspect is to be thoroughly researched.

IoT is extremely vulnerable to attacks for several reasons. First, its components are often unattended and remotely located. This gives attackers a chance for physical attacks, and it is even harder to manage security in such a case. Therefore, it is essential for security solutions to become more autonomic and to rely less on human intervention. Furthermore, systems are becoming increasingly sophisticated with arising issues of interoperability and maintenance. The complexity of heterogeneous objects would keep growing past the point of human ability to manage all smart objects. Second, IoT uses wireless technology for communication and wireless communication is easier to compromise. In general, most of the components of IoT like end devices lack high computing resources (Sehgal et al., 2012). This serves as a roadblock to the implementation of more secure and complex security protocols. A single point of failure may exist in IoT systems also. These systems can be thought of having three parts which are information collection, transmission and information processing (Mobahat, 2010). The actual architecture will vary but most certainly will have a central processing router, gateway or computer. An inherent flaw exists in such a design in the form of the sink where "*disabling it will kill the network and compromising it will result in data leak*" (Di Pietro et al., 2009). IoT components are also critically vulnerable to Denial of Service (DoS) attacks. Wireless technologies are susceptible to interference and interception as well, and a determined adversary cannot be stopped from mounting a DoS attack. Finally, the existence of man-in-the-middle (MITM) attack proves to be a problem without any solid solution.

This article aims to discuss various threat mitigation approaches related to security in IoT which follow an autonomic[1] approach. It also includes discussion for the appropriate information security model. Luckily, the conventional aspects for security in the case of WSNs are applicable here as well. The security triads of confidentiality, integrity, and availability (CIA) have been achieved by many systems without requiring significant human intervention. However, it is also required to highly consider privacy and authenticity of data in the realm of IoT. Similarly, making security decisions and providing maintenance must keep up with the deployment of IoT devices, and manual intervention would result in unnecessary slowdowns. Identifying the origin of failures and increasing system efficiency in the network would become a subject of importance as manual maintenance may not always be the best way out. Dependence on human manual intervention has to be minimized and approaches for security have to be made self-sufficient and autonomic.

Our objectives in revisiting the literature are threefold: 1) to learn how autonomic computing techniques can be applied in the context of security in IoT, 2) to build a taxonomy linking together security and autonomy, and 3) to highlight open challenges and to discuss future research directions in the field.

Section 2 introduces the elements of autonomic computing and its assumptions, followed by a discussion on the self-⁎ paradigm. Section 3 describes the most relevant security goals of the IoT information security model. Section 4 attempts to classify threat mitigation approaches according to the proposed autonomic taxonomy. Challenges and future directions are discussed in Sections 5 and 6 respectively.

2. Autonomic security

This section discusses important features, requirements and characteristics present in any autonomic system as well as the working of the core control loop in a general autonomic framework. It then introduces the concept of autonomic security by discussing paradigms of self-healing and self-protection.

2.1. Autonomic computing

Autonomic computing is a concept that "*brings together many fields of computing with the purpose of creating systems that self-manage.*" (Lalanda et al., 2013). This term finds its origin in biology (Jänig, 1989) to refer to bodily tasks which function unconsciously. Nowadays, autonomic concepts have been applied in diverse technological areas for self-management. As an example, NASA increasingly relies on the concepts of autonomic computing to increase survival rate of remote missions, where human tending is not feasible (Vassev and Hinchey, 2013). An autonomic system has also been defined as "*an intelligent system, or system of systems where data acquired by sensing or monitoring capability is utilized in an overall autonomic decision-making process.*" (Ashraf et al., 2014b).

An autonomic computing system must configure and reconfigure itself under varying and even unpredictable conditions. System configuration must occur automatically and dynamic adjustments must be made according to that configuration in order to best handle changing environments. For long term sufficiency, any network and system in IoT must achieve some sort of autonomic behavior without any human intervention. An architectural framework was proposed by Kephart and Chess (2003) to make system management easier under the vision of autonomic computing. Following this, autonomic computing was re-defined as "*a vision that enables any computing system to deliver much more automation than the sum of its individually self-managed parts*" (Koehler et al., 2003). Another goal for any autonomic system is to modularly divide roles among the constituent components without sacrificing functionality. The presence of a central authority is an imperative prerequisite and allows for controlled management of the agents involved.

Autonomic computing deals with the management of computing resources in a manner so as to minimize the user intervention. The concept of autonomy is towards deploying technology specifically to manage and optimize the functionality of other technology. The aim is to reduce the need for manual intervention in the other schemes. Relating it back to the theme of the paper, it would refer to being able that a system can adapt correctly to given stimuli, maintain key behavior and avoid harmful ones in the presence of security threats.

Autonomy is extensively described in the literature in terms of the self-⁎ paradigm. The next sub-section introduces the same, with special emphasis on the security elements of self-protection and self-healing.

2.2. The Self-⁎ paradigm

Self-⁎ (self-star) refers to the set of self-organization, self-awareness, self-adaptive, self-designing, self-building, and self-repair paradigms. The philosophy of self-⁎ seeks to describe essential qualities that should constitute the behavior of an autonomic element. This concept has been described extensively by Babaoglu et al. (2005), in which approaches are recommended to be modeled on nature, where autonomy is at the highest. Limiting the discussion to security mechanisms, the autonomic paradigm allows for the concepts of self-healing and self-protection to exist in a system:

- Ability to Self-heal: a system should be able to discover causes of failure and correct faults without human supervision. The implementation of fault detection is comparatively easier than the implementation of the exact mitigation approach needed. Nevertheless, considerable number of attempts (Zhang and Arora, 2003; Gui and Mohapatra, 2003; Poor et al., 2003; Amin, 2002; Di Pietro et al., 2008; Vlajic and Moniz, 2007; Kim and Shin, 2007; Wasilewski et al., 2007) have been made in the field of WSNs in dealing with wide aspects from routing to general service recovery. A number of studies (Dutta et al., 2007; Kausar et al., 2007; Han et al., 2009) have dealt with specific security issues, such as key distribution methods.

[1] The term '*autonomic*' refers to '*self-sufficient*' management of resources by any system without any particular intervention from a user.

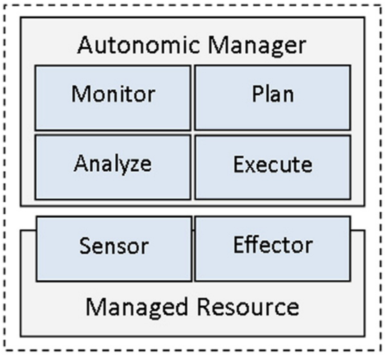

Fig. 1. Autonomic Four Part Control Loop Adapted from Kephart and Chess (2003).

Readers are recommended to read the dedicated survey on self-healing systems by Ghosh et al. (2007).

- Ability to Self-protect: a system should identify and protect its components from random attacks. Wang et al. (2008) present an approach for efficient self-protection in a static WSN. This approach may not apply to IoT, in which nodes may join and leave a network continuously. Another software model is presented by Qu et al. (2004) for self-protection, and this model shows a good level of security against few attacks.

2.3. *Autonomic control loop*

According to Kephart and Chess (2003), autonomic computing is implemented by an autonomic manager component and a managed resource component using the MAPE control loop. This MAPE control loop is more like a structural arrangement than a sequential control flow. As shown in Fig. 1, control loop architecture is divided into four separate parts on the basis of their functionality:

2.3.1. *Monitor*

Monitor module is responsible for collecting details from an element. Details include the data obtained from the environment and the data related to the element itself. This module is also responsible for the aggregation, filtration, management, and reporting of all details.

2.3.2. *Analyze*

Analyze module provides mechanisms that model complex situations based on the received details. This allows the central authority element to learn about the environment. This module can also be used to predict future states.

2.3.3. *Plan*

Plan module provides mechanisms that guide action with the help of higher level policies, rules, and regulations. This module plans further action on the basis of the constraints that have been imposed in the system. The action is performed to achieve system goals and objectives.

2.3.4. *Execute*

Execute module controls the implementation of the devised "*plan*" with support for some kind of feedback.

Autonomic implementations always require two sets of actors or agents. One is the implementation of the autonomic manager, and another the managed resource. In IoT, it is not possible to point out the best combination of autonomic agents due to the heterogeneity involved. Thus, different contexts of autonomy exist, ranging from end networks to higher layer protocols. The managed resource comprises traditionally of a set of sensors and actuators. Sensors carry out collection of raw data, traditionally limited to response times, network and disc usage, memory and CPU utilization and similar data sets (Huebscher and McCann, 2008). In the context of IoT, sensors act as the central backbone of information, sensing the environment for physical and natural data. The context of the sensed data in managed resource has shifted from server-machine-based to environmental-nature-based.

3. Information security goals

IoT is structured in three layers of perception layer, network layer, and an application layer (Zhao and Ge, 2013). The perception layer is responsible for object information, interfacing with the environment as well as origin of sensor data. Network layer handles middleware implementations and communication from network to network. Finally, application layer in IoT describes schemes for reporting, big data, analytics, user interfacing and data storage. Traditionally for each layer; the information security components, referred to as CIA, form the common security goals. However in IoT, in addition to the CIA triad, the goals of privacy and authenticity become important as well. In order to discuss autonomic security, it is important to discuss the relation of IoT autonomy with these generic information security goals.

3.1. *Confidentiality*

Confidentiality guarantees that information is not disclosed to unauthorized persons or processes during any communication transaction (Wrightson, 2012). Confidentiality is a key security feature because it ensures that only authorized nodes can get access to sensor and control data. The basic purpose of confidentiality is to ensure that data transferred from one node to another node is not accessed and understood by any intermediate node or third parties. This is usually achieved by using symmetric key cryptography where both the sender node and receiver node use a shared secret key, and the data is then encrypted or decrypted using this key (Delfs and Knebl, 2007).

Autonomy in confidentiality is an important factor for IoT as there remain many areas where autonomic decision making can be applied to one's advantage. Decisions in the realm of confidentiality that can be linked to autonomy include:

3.1.1. *Decision on storage*

The autonomic system should be able to decide dynamically about the amount of data to be stored locally based on the external conditions. Self-protection would refer to the decision of dynamically setting an optimum or minimal storage use and encrypting the storage for confidentiality. Self-healing would be the ability to re-generate lost data, or recover from an event of memory abuse/memory full.

3.1.2. *Updating of security keys*

The autonomic system should be able to manage any security keys for local use in the system. It should constantly be able to monitor, and prevent an instance (self-protection) where communication confidentiality can be compromised. In the event of security breach, the system should be able to switch into a fail-safe mode, or generate/fetch new keys (self-healing).

It is important to take note that asymmetric cryptology for confidentiality such as public key infrastructure based encryption schemes are resource exhausting. IoT includes elements that are extremely constrained in terms of energy, and computational power resources (Sehgal et al., 2012; Gluhak et al., 2011). Addressing these constraints, a few light-weight key management schemes are still under development and require large research efforts. The main research challenges when it comes to confidentiality are to develop autonomic versions of the approaches and systems which complement identification models for individual nodes. These should take into consideration the problems of energy consumption, computational power, memory resources, as well as the aspects of organization and communication. Indeed, IoT devices readily support symmetric schemes with acceptable overhead[2] for achieving the goal of confidentiality of sensor data. On the other hand, asymmetric encryption is used only for specific events such as initiation or key-distribution, and not to encrypt sensor or context data.

3.2. *Integrity*

Integrity refers to the inability of modification of information by unauthorized users (Wrightson, 2012). Confidentiality, as previously discussed, ensures that data originates from an authorized source. Data integrity solutions, however, guarantee that an adversary cannot modify data in the transaction without the system detecting the change. This is typically solved by using symmetric cryptography which helps to create signatures corresponding to the data under transmission. Signing individual data messages using asymmetric schemes is impractical and slow. In IoT, asymmetric schemes are mostly employed for securing the initial process of symmetric key exchange, except for few schemes such as by Vucinic et al. (2014). The rest of the communication process employs symmetric cryptography which is less resource intensive. Signatures are prepared by the sender and sent through the transmission media. The receiver verifies the signature and hence confirms that the data was, in fact, actually sent from the authorized node. It can also be achieved by use of message integrity code (MIC) or a checksum added to each packet. MIC can detect message altering caused by accidental transmission errors as well as malicious altering. Checksum on the other hand can only detect accidental transmission errors. Example of attacks on integrity are tampering and spoofing. Typical cryptographic techniques spend large amount of resources in terms of energy and bandwidth both at the source and the destination.

Autonomic solutions are required which should be able to provide a satisfactory level of security regardless of the scarcity of resources. Autonomy in integrity includes decision making components such as:

3.2.1. *Logging data alterations*

The autonomic system must be able to generate enough logs to reveal the path of data alteration in case such an event is observed. The decision will be whether to store these logs locally or centrally, as well as the duration to save the logs. There may exist two levels of log keeping; one for the end devices, and another for the system as a whole.

3.2.2. *Integrity of device software*

The autonomic system should make sure that all devices will run only authorized software. The system should be able to monitor the event when a device is captured and floods the network with pseudo-data. Self-healing will allow the system to ignore any data generated at the device as well as notify the user to take appropriate actions.

3.3. *Availability*

Availability ensures that a system's authorized users have timely and uninterrupted access to the information in the system (Wrightson, 2012). The whole system along with all its components should be functionally available, and capable to provide their services whenever required. This includes properties of scalability and survivability. Attacks on availability include DoS, jamming and malware. An attack on availability takes on a new meaning in IoT as DoS attacks could physically harm the nodes. The node could be "*killed*" by depleting its energy resources. Constant queries from an adversary to an IoT device to force it to respond can make the device run inefficiently and exhaust its battery resources in a much shorter time. Research is needed to address these issues and models required to prevent and even recover the IoT system in the event of an attack on the availability.

3.3.1. *Fault tolerance*

In case a failure or attack occurs, self-healing systems should be able to deliver the lowest level of functionality.

3.3.2. *Scalability*

An autonomic system should be able to expand smoothly in the event of introducing extra resources. A lot of research in IoT addresses the scalability issue. Autonomic decisions may include deciding on duty cycling methods, where part of the network can be switched off without losing functionality. Here, the system will not only protect the availability but also help in prolonging the lifetime of the network. Similarly, availability is important in the event a large number of nodes attempt to enter a network simultaneously. Here, the system can automatically decide on contention parameters, such as done by Ashraf et al. (2014c).

3.4. *Privacy*

Privacy defines the rules under which data referring to individual users may be accessed. Some of the research (Kalloniatis et al., 2008; Coen-Porisini et al., 2010; Lioudakis et al., 2007; Sweeney, 2002a; Bhargav-Spantzel et al., 2007) has focused on security frameworks for privacy issues at a high level of abstraction. These are suitable only at the application layer. This is mainly because different IoT systems may have different requirements for privacy. One method worth mentioning has been proposed by Lioudakis et al. (2007) where a proxy interacts with a user on one side and the services offered on the other. This method guarantees the least required amount of information be made obtainable depending on the preferences set by the user. Such a solution while innovative is not suitable for the IoT. In the context of scalability, it would be physically impossible to set preferences for such a huge set of nodes. The need of the hour is to develop privacy models while keeping in view the immense scalability of the nodes and variability in terms of IoT applications. The privacy policies should complement identification models for individual nodes and should give some amount of control to the user, if not all. Identity management is also a problem related to IoT device privacy (Vidalis et al., 2014). Wei et al. (2014) implement privacy by batch verification, as well as prioritizing computation, auditing and analysis. Previously, concerns of cloud security are restricted to storage only (Wei et al., 2010). In IoT, such cloud layer applications can be included into the autonomic system to allow for greater compatibility.

Privacy could be considered as a sub-set of confidentiality. The reason to keep it separated is because privacy also refers to non-linkability, location privacy, context privacy, trust management and most importantly anonymity. The goals of privacy are categorized into the following based on the context of the private data under consideration:

[2] Thanks to the paper reviewers for highlighting that.

3.4.1. Non-linkability

It refers to the division of private data for the same user so that no one can establish a profile based on the data. For a single user who owns a multitude of devices, the autonomic system should be able to dynamically add noise to the data, and then be able to filter it out as well. This will prevent any attacker from searching for patterns and reverse engineering any sniffed data. The disadvantage of such a method, however, is the increase in the data bandwidth that is required. Nevertheless, the decision on the optimum amount of addition of data noise, as well as the frequency is another responsibility for an autonomic system.

3.4.2. Location privacy

It guarantees that a device's current and past location is not disclosed.

3.4.3. Context privacy

In context privacy, access context information should be kept secret. Self-protection of personal information, as well as the type of data that can be generated and processed at the device should be ensured. In an example concerning medical IoT systems, there may be different profiles of context privacy to access patient data without explicitly requiring patient's permission (Ashraf et al., 2014a).

3.4.4. Anonymity

It demands the identity of a node be hidden. This results in a direct consequence for location privacy as well. A purely anonymous communication is needed because of shortcomings of existing communication protocols.

3.5. Authenticity

The goal of authenticity guarantees the legitimacy of the parties under consideration since it is necessary to ensure that communication data should actually origin from where it claims to origin from (Grover and Lim, 2015). Similarly for IoT, it is also important to validate the parties involved in M2M communication, while keeping IoT constraints in mind. Recently, a light-weight authentication protocol was proposed to replace complex encryption algorithms by adopting a hardware approach (Lee et al., 2014) to address the device constraints. Moreover, a significant advantage for authentication schemes is IoT is that they can benefit from innovations of device specific features such as near field communication (NFC) tags, RFID tags, as well as location based information. As an example, Petrov et al. (2014) propose a NFC based authentication using an innovative way to tackle the problem of constrained resources in IoT. Their scheme utilizes passive NFC so that battery and computational resources are not employed at the end devices. Traditional authentication schemes may even lead to novel challenges in IoT, e.g. Mahalle et al. (2014) suggest that authenticating individual devices in a short time is impractical, and propose a group based authentication scheme to overcome the associated problems. Furthermore, bio-metric authentication schemes such as finger-print recognition are not applicable for IoT devices (Ren et al., 2013). The requirements for autonomy in authenticity need to consider MITM authentication, trust management and monitoring functional states:

3.5.1. MITM authentication

Many attacks target confidentiality in an attempt to get access to the data. These include but not limited to eavesdropping, traffic analysis, cloning, replay, spoofing and MITM attacks. The MITM attack is a form of active eavesdropping in which the attacker acts as a router and makes independent connections with the targets and then transfers messages between them. A MITM attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other. Self-protection for an autonomic system would refer to the methods of prevention of impersonation of any device. Thus, the system should be able to dynamically modify the identity information for a given device, as static identities are easier to impersonate. Impersonation makes the end nodes to believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. In the conventional Internet model, most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. Various defenses against MITM attacks use authentication techniques that are based on public key infrastructure, secret keys, mutually trusted certification authorities, latency examination, channel verification, and one time pad. MITM-attacks are a problem without any solid solution, the root cause being that authentication is a problem without a solid solution. An autonomic self-healing system can dynamically switch and use different methods after an MITM attack has been observed. Prevention of MITM attacks can be only achieved by employing strong authentication techniques as well as solving trust management problem.[3]

3.5.2. Trust management

A large scale adoption of IoT is proportional to the security offered by IoT services. Trust is one important factor which helps customer acceptance as well as reduce the element of risk. Few schemes do exist where IoT components interact solely based on trust, such as adaptive routing in a smart grid (Xiang et al., 2014). An early attempt towards autonomic device management considering trust requirements is also available (Hammer et al., 2014). In one case, not only does trust based methodologies contribute to security, but network performance was also found to be improved (He et al., 2012). Readers are recommended to refer to the publication by Yan et al. (2014) on trust management for IoT.

3.5.3. Monitoring functional states

In addition to the sensor obtained data in IoT, control data such as to monitor the functional states of any system also needs to be authenticated. Monitoring as a pre-requisite process in autonomic algorithms could be applied for 1) detecting device faults, 2) detecting configuration changes, and 3) collecting performance data. Here, authentication provides the means to verify the identity of a node that participates in such monitoring tasks (Battat et al., 2014).

4. Threat mitigation taxonomy

As highlighted earlier, security solutions have been classified as either self-protecting or self-healing, in relation to the autonomic mechanism used for mitigation. Self-protecting solutions follow a passive approach and attempt to prevent security threats before they happen. This is done using various cryptographic techniques, with the knowledge of how common attacks are executed. In the case of self-healing solutions, the specific counter-measures for mitigation are taken only after the attack has been detected. Reactive measures are easier to achieve than protective measures, as typically the attacks aim confidentiality, integrity, availability, authenticity or privacy. Nevertheless, it is important to include protective mechanisms as well supplementing the reactive mechanisms, resulting in what we call as hybrid schemes.

Threat mitigation solutions have been classified separately according to layer based, actor based, and specific approach methodologies.

[3] Thanks to the paper reviewers for the highlighting that.

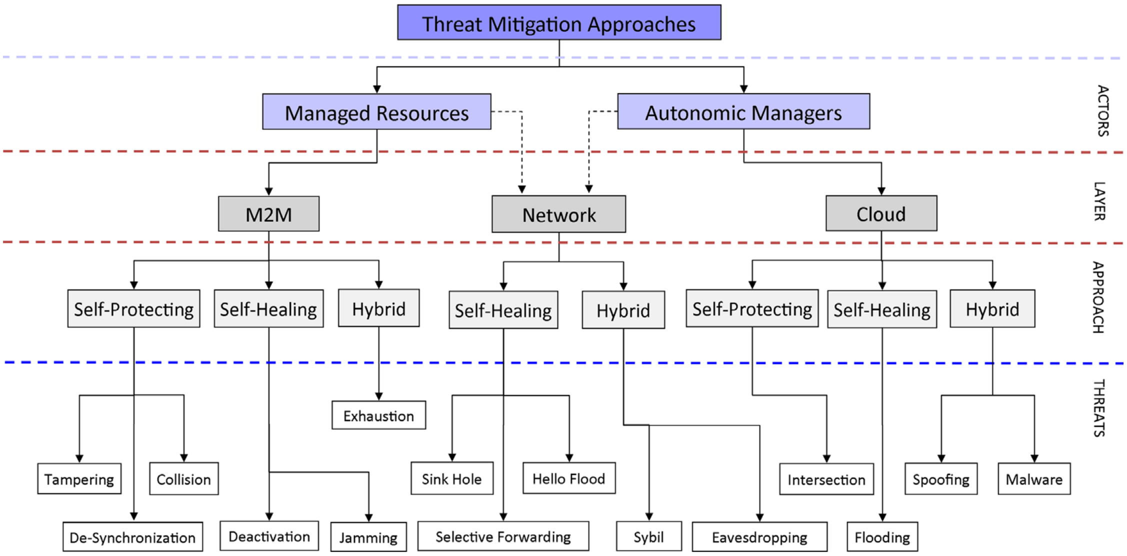

Fig. 2. The proposed taxonomy for security threat mitigation techniques. Research works may be classified under one or multiple categories.

The solutions which aim to solve specific layer-based problems have been grouped accordingly. All layered classifications have been further grouped loosely based on autonomic activity as either autonomic managers or managed resources. Due to the absence of a clear line of defense, a complete security solution should integrate both self-healing and self-protecting approaches, and should be able to prevent, detect and then react appropriately. As threats become faster and more aggressive, so should the responses.

The proposed taxonomy is summarized in Fig. 2 and discussed in the following sub sections. In this proposed taxonomy, mechanisms residing in the managed resource and autonomic manager will be further classified as M2M, Network, or Cloud based. More particularly, the proposed taxonomy aims at grouping IoT security vulnerabilities and their mitigation solutions using an autonomic terminology.

4.1. M2M layer

The most effective implementation of autonomic security approaches is possible at the M2M layer as hardware based solutions are more robust and faster than software based ones. One such example is a light weight authentication scheme proposed by Lee et al. (2014). To keep the cost of the end devices low and achieve long battery life, complex schemes are usually avoided. Attacks in the M2M layer include jamming, deactivation, tampering, collision, and exhaustion which have been described next.

4.1.1. Jamming

Jamming is an attack on availability and renders the wireless spectrum to be unusable for the constituent devices. The threat level from jamming based attacks can be considered very high in IoT due to the characteristic of remote, unmonitored deployment of IoT devices. Jamming mitigation approaches fall traditionally under self-healing paradigm. Jamming is classified as a physical layer attack in which the radio frequencies are disturbed by use of interference and saturated with noise signals which effect the transmission of legitimate signals. Signal jamming of radio frequency channels results in a DoS attack and is prevented by a proper monitoring of cognitive spectrum (Liu et al., 2013), and eventually distributing the usage across the available spectrum.

In the popular techniques of jamming mitigation, autonomic behavior is manifest and can be further developed as follows. Wireless sensors such as sniffers usually collect details about Received Signal Strength Indicator (RSSI) values and similar wireless information from the environment. This represents the "*Monitor*" phase of the MAPE architecture. These details are compared with known patterns and extreme values for specific parameters, such as an abnormally high RSSI values in a specific frequency of the spectrum. Once a possible jamming attack is suspected, the appropriate mitigation method is planned, and then executed by the effector. In the technique by Liu et al. (2010), instead of monitoring the RSSI values, analysis of the hearing range of the wireless nodes inside the jammer area is done. The execution of mitigation can follow different forms as well. Some methods attempt to neutralize the jammer signals by cancellation (Shoreh et al., 2014) and by switching the usage in other portions of the spectrum (Kang et al., 2013), whereas some merely attempt to localize the jammer for further action (Cai et al., 2013; Habaebi and Ashraf, 2014). Some methods are also specifically designed to cater for problems in specific access control methods. As an example, DEEJAM (Wood et al., 2007) attempts to mitigate jamming attacks specifically in IEEE 802.15.4 standard based wireless networks.

4.1.2. Tampering

Tampering is essentially an attack on confidentiality and availability. Data tampering occurs when an attacker modifies, adds, or deletes data in the end device itself. In such attacks, the end device is compromised by physically capturing a node from the network. The attacker can collect all information and try to recover beneficial information. An advanced attacker can recover, reprogram and redeploy it in the field to attack the network. An attacker can study the type and format of data that is being transmitted by IoT devices, and attempt to tamper and generate the same. In such a case, the accuracy of the data generated by the network is questionable. An autonomic scheme for self-protection based on device identities, and proper authentication, is needed to preserve the integrity of data.

The MAPE architecture can be implemented as follows. The system can monitor for suspicious data being generated by the nodes, and periodic checks could be made to see whether the node has been compromised. Based on this control data, the system can mitigate it by dropping the data generated by the suspicious node. For example, if the system detects possible capture, it may remotely instruct the node to delete any data stored on the device, such as security keys and synchronization data. This can significantly delay and prevent attempts at reverse-engineering. In the scheme by Henrici and Muller (2004), the primary concept is that neither the keys nor any usable data are stored on a RFID tag, and thus capture of a node will results in little or no damage to the system. Tampering is classified as a low threat category, but highly affects the integrity of data.

4.1.3. *Deactivation*

This refers to the physical destruction of the node or unauthorized application of a "*kill*" command. Deactivation results in loss of availability in the network. We can imagine the following scenario to appreciate the need of mitigation methods against deactivation. Smart cities are filled with IoT devices, to sense and actuate, and are in the danger of being destroyed or stolen by people. This can re-define modern day cyber vandalism to a new level. An attacker can also attempt to enter the interface of the node, and try to shutdown, or kill the device. From network's perspective, both these attacks will lead the node to stop being detected, and cease to function. Password protection as well as physical security measures such as camouflage can provide some respite. However, a large scale application of this attack will result in the network falling apart and perhaps DoS may result in multi-hop environments.

Deactivation can be classified as a high impact attack in the wisdom that perhaps there are no software methods that can effectively prevent it. Remote triggering of the kill command can be disabled, but a physical damage cannot be. The only way out is to protect the node from external influences by enclosing in a protective case. Monitoring the status of IoT devices is important, which also includes monitoring the physical condition of the nodes. It may be argued that autonomic computing does not exactly fit as a possible solution for this attack, as the scope is more physical and is not affected by software mechanisms. However, monitoring the status and analysis of such data could help the user reduce the downtime of the system. The MAPE architecture could monitor the loss of any node, and then assign its offered services to some other node in the network, such that overall service levels are maintained. That would be one manner, where self-healing could be demonstrated for deactivation.

4.1.4. *Collision*

Collision is similar to the jamming attack, as the loss of data packets happens by virtue of simultaneous existence of signals in the concerned spectrum. Collision may also occur intrinsically in a large network, due to problems in the design of synchronization and transmission times. Transmitted data packets can be disrupted by the malicious users transmitting asynchronously that can result in a checksum mismatch or back-off in some MAC protocols. An attacker listens on the communication medium and guesses the expected time of message transmission. The attacker then sends a message at the same time when a proper message is started which results in collision of the message in the wireless medium. Repeated cycles of collision can result in a DoS attack and affect the availability. In IoT, there is a high probability of collision due to co-existence of many protocols in the WIFI 2.4 GHz band (Howitt and Gutierrez, 2003).

Monitoring RSSI values such as in jamming mitigation is not of much use, as attacker's signals are more dynamic and stealthier. An autonomic system can recover by dynamically adapting with a variable flow control mechanism for collision mitigation due to a jammer (Hang et al., 2013). Autonomic self-healing for collision recovery by random number based mechanisms could be a future research area.

4.1.5. *Exhaustion*

Exhaustion results as an after-effect of some of the previously mentioned attacks. Devices on batteries can be energy exhausted if the network faces continuous collisions and DoS attacks. In many M2M MAC layer protocols, collision results in repeated attempts at re-transmission, which highly drains the battery resources. Solutions of rate limitation and a timer can help prevent exhaustion in end nodes. Exhaustion could be a result of other attacks, which aim to exhaust the energy resources. Exhaustion is classified under DoS for high impact attacks and has been linked to the deactivation attacks. The linkage is due to the common pattern of the permanent removal of nodes from the network with a common goal to reduce the network size.

Common mitigation methods include rate limitation, use of timers, cognitive adaptation, as well as cross layer designing (Feng et al., 2013). Autonomic decisions may include deciding on duty cycling methods and cognitive adaptation. The system will not only protect the availability but also help in prolonging the lifetime of the network.

4.1.6. *De-synchronization and replay*

Request for retransmission of missed frames can be made by repeatedly forcing messages into the network which carry sequence numbers to one or both end points. Time Division Multiple Access (TDMA) based schemes are particularly vulnerable and few countermeasures are explained by Manzo et al. (2005). In this scenario, separate methods exist for single hop networks and multi-hop networks. Replay is mostly an attack on synchronization whereby an attacker stores previously transmitted data and repeats it at a later time to mislead the receiver node. Many authentication mechanisms such as by Corson and Macker (1999) are immune against the replay attack, and lessons can be learnt in order to design an autonomic secure system. Simple encryption of data can also be an effective means against the replay attack. Replay attack could thus be considered as the easiest attack to be mitigated. It has been placed in a high risk category as failure of mitigation can lead to the downfall of the efficiency in the network. Mahalle et al. (2014) mitigate the replay attack by dynamically changing the session key upon fulfillment of certain conditions.

4.2. *Network layer*

4.2.1. *Hello flood*

Some routing protocols require nodes to broadcast hello messages to announce themselves to their neighbors. A node which receives such a message may assume that it is within a radio range of the sender and attempt to use the route as a communication path. However an attacker with large enough transmission power could convince every other node in the network that the attacker is its neighbor. This will lead to far away nodes sending the packets to the attacker which will be lost. The work by Singh et al. (2010) presents some counter-measures. This is a fundamental issue when it comes to acknowledgment based systems. However, acknowledgments are usually in the dominion of a powerful host with sufficient energy resources. For routing mechanisms, unequal transmission radii of legitimate nodes may also result in a hello flood. This attack has been classified as a low impact attack on availability. Autonomic mitigation mechanism may include use of authentication, and puzzle schemes such as described by Koh et al. (2013).

4.2.2. *Sinkhole*

An adversary attracts a central node and compromises it leading to loss in availability. This leads to message drops and even a DoS attack. An intrusion detection system (IDS) is described by Krontiris et al. (2008) particularly to detect the sinkhole attack for the MintRoute protocol. Furthermore, the IDS by Choi et al. (2009) is able to detect the sinkhole attack for networks using link quality indication (LQI) based routing protocol. An autonomic system, however, demands reactive measures to be taken once the detection has occurred. The risk level in this case is very high as compared to the tampering attack where just a handful of end nodes are compromised. Not only can all the data be sniffed, but the network could be controlled if it is infrastructure based. Autonomic methods may include the use of distributed architecture and use of authentication (Shafiei et al., 2014).

4.2.3. *Sybil attack*

In a Sybil attack, a single node creates its own multiple identities and presents it to other nodes in the network using them to gain a disproportionately large influence. This will result in removal of all original neighbors from the table of active sensor nodes in the routing table. System's vulnerability to a Sybil attack depends on how easily identities can be generated. It also depends on the degree of reputation to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity. The local Sybil resistance scheme (LSR) attempts to detect Sybil attacks particularly in the use case of vehicular networks (Lin, 2013). Vehicular networks seem to be the hot topic as a use-case for research in Sybil attacks. Lin (2013) also discussed the availability of a road side unit (RSU) to help counter and detect the attack. Work by Zhou et al. (2011) also focuses on vehicular networks and aims to detect the Sybil attack through a distributed, workload and passive overhearing. They attempt to preserve privacy while doing the same, and claim minimal overhead and network delay.

The work by Yu et al. (2008b) discusses three requirements for defenses against a Sybil attack in a vehicular network. First, any proposed scheme should protect the information about the nodes, and thereby preserve privacy. Second, the response time of the counter measure should be immediate. Finally, a verifier should be employed to prevent the Sybil attack to automatically adapt towards the prevention schemes. Lessons from autonomic computing can contribute highly to the third requirement. They propose SybilGuard which portrays the use of these requirements and sets a limit to the number of false identities that can be initiated by a malicious user. SybilLimit is proposed by Yu et al. (2008a) from the same research group, which improves upon the concepts set by earlier by adopting and including a social based setup. Mobility is considered by Lin (2013) and by Zhou et al. (2011) specifically in the case of vehicular networks in the form of moving cars etc. The work by Abbas et al. (2013), however, presents a light weight scheme, residing in the lower layers; with support for mobility and variable transmit powers as well. The detection is based on rules such as the rule for values of RSSI for new nodes that attempt to join. This mechanism, however, might not apply in all cases as the analysis is solely on the first RSSI values, which a knowledgeable, powerful malicious node might easily bypass.

4.2.4. *Selective forwarding/gray hole*

Certain malicious nodes can refuse to forward some messages and just drop them. This can result in delay and bandwidth degradation in the whole network. Thus, confidentiality and availability are compromised. Probing and redundancy checks can be the possible solution. Many solutions have been proposed which range from providing detection to a complete recovery. Others focus on lessening the damage caused. A scheme which detects and recovers the network has been proposed by Deng et al. (2009). With a claimed accuracy of over 95%, the scheme employs a messaging based watermark technique to keep track of the forwarded path. This scheme however, claims to result in network delay due to the cost of processing. The work by Shila and Anjali (2008) focuses on the Ad Hoc On-Demand Distance Vector (AODV) and similar routing protocols before proposing a scheme that consists of two phases of detection and localization. They use packet counters to keep track of a series of control messages which are passed through the wireless nodes. Another method termed CADE, also makes use of acknowledgement based detection but eliminates time synchronization requirements (Kim et al., 2008). CADE makes use of cumulative techniques and claims to reduce overhead. Another technique by Pandarinath (2011) breaks the information packets into a multitude of smaller pieces, propagated along specific paths and then the decision of malicious node presence is made. A complete survey on the proposed solution for this attack has been conducted by Bysani and Turuk (2011). The common mitigation measures which can benefit from autonomic practices include probing, redundancy, and message based detection (Mohebi and Scott, 2013).

4.2.5. *Eavesdropping and traffic analysis*

The eavesdropping attack and traffic analysis act as a pre-requisite to many other attacks, and usually the transmitter and the receiver are unaware of the presence of this attack (Dai et al., 2013). Eavesdropping and traffic analysis are classified as either passive or active. In passive eavesdropping, the attacker detects communication traffic by listening to the transmission medium, and processes it to extract vital information. On the other hand, in active eavesdropping, the attacker sends control data as queries to initiate specific processes and replies from the destination device. The reply is further used in the analysis to pave the way for other attacks. It is hard to decide on whether eavesdropping should be grouped under M2M, Network or Cloud attack since data can be eavesdropped at levels of communication. Eavesdropping on data in the M2M layer is easy, but not as beneficial as the adversary can only eavesdrop on selected portions of the system, and the raw data may not be particularly useful (Rabbachin et al., 2011). Wireless IoT devices are heavily prone to eavesdropping. On the other hand, eavesdropping on data in the Cloud layer is essentially the most profitable, as context information is included as well. However, the ease of implementing an eavesdropping attack on the Network layer makes it suitable for this category. Eavesdropping could be active or passive, depending upon whether the sniffed data is just monitored for information, or used for initiating another attack. The MITM attack, discussed earlier, is an example of an active eavesdropping attack. Here, the adversary makes independent connections with the source and destination devices, acting as a router, and transfers messages between them. In this process, data is captured, understood and modified. Eavesdropping on a new device that is attempting to join a network may allow the attacker to observe control data. This can further allow the attacker to generate messages impersonating other devices, and to manipulate and understand how the network topology is built (Pawar et al., 2011).

4.3. *Cloud layer*

4.3.1. *Flooding*

The attacker can exhaust important resources like battery by sending the victim many connection establishment requests. Ad hoc layers have received some attention for mediating the flooding attack in (Ping et al., 2006). Here, Ping et al. present an ad-hoc flooding attack that aims to exhaust node resources and bandwidth. The corresponding proposed solution is able to recover bandwidth automatically and save resources but may not be able to stop the interference caused by the intruder broadcasting continuously. Flooding has been linked to hello flood based attack as they resemble in the methodology for attack. Furthermore, this has not been classified as a high risk attack as IoT end device will be rarely employing transport layer based advanced mechanisms of TCP. UDP instead is not highly vulnerable as connection is not established. IoT communication within transport layer is expected to be majorly connectionless. This attack on availability can be easily mitigated by setting traditional connection establishment barriers as a part of autonomic self-protection measures.

4.3.2. Malware

This is an attack on confidentiality of information. Malware traditionally refers to the application of viruses, worms and Trojans to interfere with the system. Malware attacks have been included in this study as vulnerable mobile phones and other high end devices are also a part of the IoT. Malware may not affect the sensor based motes but significant risk may exist for sinks/gateways being represented as applications in the mobile phones. Bluetooth devices may be at risk more than the other technologies such as 802.15.4. Mitigation solutions include constant vulnerability scans using malware pattern classification (Canzanese et al., 2013) and risk mitigation services (Loveland et al., 2008). The pattern classification can be done using the autonomic control loop component of "*Analysis*" following which the autonomic "execution" of the mitigation service can be performed.

4.3.3. Spoofing and message forging

Spoofing occurs when an attacker successfully impersonates a node. A data transmission may be recorded from the node by someone with a suitably programed portable reader. During retransmission it appears to be a valid node. However it is not to be mistaken for *cloning*, as there is no actual node involved, just a much bigger and powerful portable machine. Spoofing has been classified as a high level risk because of the method of the attack. Spoofing attack may not just be limited to the application layer, but can exist in all layers. Spoofing is an attack primarily on authentication, and impersonation of nodes defeats the principles of privacy as well (Schaffer et al., 2012). For IoT, research is needed to mitigate the spoofing attacks in an autonomic manner. Message forging, on the other hand is can attack where the adversary creates a new message or modifies an existing message to deliver different content. In the specific case of modification of synchronization messages, message forging can be considered as a form of the replay attack.

4.3.4. Intersection

The intersection attack, also known as the composition attack is focused on defeating the privacy of the system by focusing on auxiliary information of a system (Ganta et al., 2008). This information is gained from other channels such as web or third part public records. It targets the non-linkability element of the privacy information model. An adversary makes use of anonymized data from different sources, and attempts to link them. Schemes such as by Sweeney (2002b) exist based on "k-anonymity" techniques to mitigate the effect of the intersection attack.

5. Challenges for implementation

It is generally accepted that horizontal, layered autonomic solutions are easier to design and develop, catered for specific security issues. However, some attempts at defining vertical security architectures have also been made. There are also few others, that provide a pattern based solution for similar attacks. Various approaches have been reviewed and discussed by (Ning et al., 2013) dealing with key distribution schemes, smart grid security, and a scheme for multimedia traffic as well as catering to the vertical idea of "*Smart Community*". However, in addition to those, other policies and approaches have also been mentioned. The challenges for implementation are summarized below:

5.1. Privacy and wireless constraints

To prevent deactivation of nodes, the kill command should be disabled or password protected. However, option of disabling will help enforce consumer privacy, so the latter solution is emphasized in any autonomic decision. A privacy protecting scheme by Juels et al. (2003) proposes IoT devices to be either private or public based in an attempt to prevent unwanted scanning of nodes. Another interesting idea by Ohkubo et al. (2004) is regarding identification of devices, in which each device will be given a temporary ID to be used in communication, so that an adversary cannot know the real ID of the node and thus privacy is protected. Privacy and trust management come complementary, and it is also another challenge to develop trust models (Gu et al., 2014).

Another idea by Juels (2005) suggests that a device can dynamically release some random information for each new gateway query, which should be used specifically by the gateway in future communications. This will prevent any attacker to impersonate the gateway node and attacks such as spoofing and MITM can be avoided thereby fulfilling the goal of self-protection. Some other approaches also make use of hashes (Ohkubo et al., 2004; Weis et al., 2004) in which the hashes are calculated at the central router or node. While this does solve the problem of the end nodes being computationally weak, however, a new problem arises that the load on the central device rises linearly as the number of nodes attached is increased. Such scalability can result in a loss of availability. In cryptography based solutions, an important scheme worth mentioning is elliptic curve cryptography (ECC) and its derivatives which have an important advantage of less memory consumption. With regard to detecting and blocking malware, it is impractical, reactive and often it is much cheaper and effective to be proactively be running periodic scans and consequently taking action as soon as possible. In this case, self-protection is more advantageous than self-healing.

Recently, Riahi et al. (2013) proposed an approach based on a cognitive and systemic approach and divides the problem from the view point of the different actors which interact with the system and the environment. In another proposed framework, Altolini et al. (2013) argue about the importance of starting from scratch and defining the software and hardware components for security. Embedded security should focus on the building blocks of approaches, secure storage, protection of hardware input/output interfaces, and even secure boot up.

IoT is largely made up of wireless networks with an extended access to the Internet that acts as the backbone for communication, hence, resulting in a fundamental vulnerability. In some systems, each mobile node in a network may function as a router and forward packets for other nodes (Corson and Macker, 1999). The important point is that the wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in wireless networks from the security design perspective.

The boundary that separates the inside network from the outside world is blurred. There is no well-defined place/infra-structure where a single security solution may be deployed. Multiple networking entities share the wireless channel and as a result the bandwidth is constrained. 6LoWPAN, for example, provides a solution in the form of relating to some security issues as well as the major issue of unique addressing of nodes. 6LoWPAN offers link layer security in the form of 128-bit AES encryption in IEEE 802.15.4. It should be noted, however, that any communication beyond 6LoWPAN routers is vulnerable (Shelby and Bormann, 2011).

The IEEE 802.15.4 has been used to implement IoT in many cases, due to advantages of low cost and power management to ensure low power consumption, along with low data rate of 250 kbps, 40 kbps or 20 kbps. There still exists a tradeoff though, in terms of performance, cost and security as can be seen in RFC 4919 that the *"the devices*

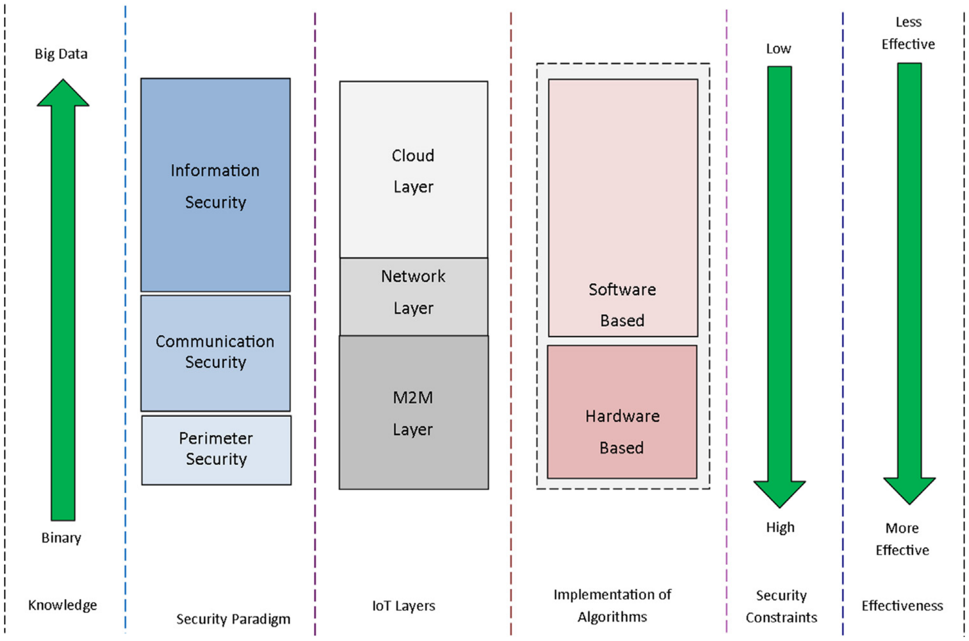

Fig. 3. Patterns observed across various layers in IoT communication

employing IEEE 802.15.4 radios will be limited in their computational power, memory, and/or energy availability" (Kushalnagar et al., 2007).

The advantage of mobility in IoT brings new challenges in which the major threats are data interception and identity forgery. The adversaries may actively manipulate, misrepresent, and intercept data, or passively monitor data transmission. For instance, in Zigbee based networks, the sensor nodes and sink nodes are dynamically self-organized in a multi-hop manner, and the malicious nodes may be embedded into the area to communicate with the neighbor nodes for data collusion.

5.2. *Architectural patterns*

Software architecture proposed by Fischer and Gesner (2012) mention how existing technologies mostly protect systems that are non-IP based, by restricting specific components using a preset rule. They provide the general requirements for fulfilling a modular, secure IoT based setup in an industrial environment. The work by Zhang et al. (2011) has attempted to develop a strategy of dividing IoT into three layers of perception, transport and application. The choice is justified based on the human nervous system layers for environment perception, signal conveyance and higher level processing. The work also evaluates the security in the layers of IoT using a weak fuzzy analysis argument. Altolini et al. (2013) recommend that software based security implementation should be avoided as they affect the overall lifetime of the network severely up to 25%. The hardware implementation would be substantially fast, as it has been proven from comparisons between hardware and software implementation of the AES security algorithm. Other works on middleware based frameworks have been reviewed by Chaqfeh and Mohamed (2012). One approach makes use of wireless scenario to the advantage of designing random implementation for wireless security (Xiao et al., 2010). An interesting work gives rise to the concept of punishment and incentive based methods, where the goal is to encourage cooperation between components and prevent selfish methods. Such methods can be grouped as soft security mechanisms (Wang et al., 2011).

In our taxonomy, the perception and the application layer have been represented, respectively, as the M2M layer and the cloud layer. This naming enables a larger scope and connects well with IoT paradigm, cloud computing and big data principles. Intelligence and big data processing takes place in the cloud layer, as well as analytics and reporting. Transmission is handled by the network layer relying on IP based communication. In the M2M layer, the devices interact with the environment, and communicate with similar devices on a low level of communication. Security constraints become higher as you move down, because of the increasing amount of heterogeneity, as well as the device limitations in processing and protection. Performance wise, lower layers are more effective as hardware implementations in security are more robust, and hard to compromise. In theory, implementation of security approaches is most effective in the M2M layer.

5.3. *Conflicting objectives*

Autonomic authentication demands an end device to dynamically reveal its identity to some extent, whereas privacy lays strict rules against any sort of identification, and disclosure of personal data. These security goals of authenticity and privacy tend to conflict, but are not exactly the opposites. Their relationship is more complex, because the more private data that is disclosed, the easier it may be compromise the authentication of a system (Chen and Nguyen, 2008). Furthermore, the broader the scope of the authentication system, the greater is the potential impact on privacy (Millett and Holden, 2003). To design an autonomic authentication system for IoT, decisions for device identifiers has to be made, such that the basic goal of authenticity is achieved. However, such decisions will have implications for privacy, and it should be ensured that device identifiers must not be easily linked to an individual user or any physical entity in the complete IoT eco-system.

5.4. *Summary*

The mentioned characteristics are summarized in Fig. 3, which reveal patterns and relation between different security concepts. Furthermore, the general challenges of security in IoT can be summarized as follows:

- Components are often unattended and remotely located which may result in physical attacks.

- For communication, wireless technology is more popular than wired connections. Security in wireless communication is easier to compromise (Sexton et al., 2009). Wireless technologies are susceptible to interference and interception as well.
- Due to the fewer high computing resources in the IoT nodes, a roadblock exists to the implementation of secure and complex security protocols.
- A single point of failure may exist in IoT systems. In the form of a central processing router or computer. Compromising that point e.g. by DoS attack can severely affect the functionality of the network.
- The existence of the MITM attack proves to be a problem without any foolproof solutions (Carmilema et al., 2012). Impersonation of each endpoint can lead to a successful MITM attack. MITM attacks can be greatly mitigated by addressing the underlying issues of authentication and trust management.
- Finally, a complete autonomic security framework should provide defense against skimming, eavesdropping, traffic analysis, spoofing, cloning, replay and MITM attacks.

6. Future directions

So far we have provided an overview of the key security issues related to the development of autonomic IoT with emphasis on the issues that require further research. Indeed, current technologies have made IoT feasible but security remains a big concern. The current literature and research activity also point to an increase in complexity and diversity in IoT in the years to come. System deployment covering across the layers has already begun in full fairness. Some of these trends will help complicate the threat mitigation approaches in the future, and demand superior autonomic independency in the systems. Such future directions have been compiled next.

6.1. *Autonomic software proliferation*

Middleware solutions allow for the rapid development and deployment of solutions. All data in IoT will have to pass through middleware deployments in order to enable compatibility across its heterogeneous components. Autonomic configuration management and dynamic service delivery require additional security schemes to reach goals of the standard information security model.

6.2. *Device constraints*

Currently, the end devices are designed to merely collect and forward sensor data to the higher layers. Increasing complexity will allow autonomic self-configuration and actuation of these devices. It is critical to protect misuse of such configuration by adoption of proper security schemes in communication and data privacy. Future devices will allow for self-maintenance thereby fulfilling another goal of an autonomic system.

6.3. *Design complexity*

Security schemes may be combined with other common research ideas in IoT, such as energy conservation. The integration and specification of security requirements for cross layer designs could be an interesting field of future research. Self-adaption and cognitive features will bring extra complexity to the system design, and security would be deemed a high requirement. Furthermore, a lighter, portable but more robust security mechanisms are also needed that take into account the level of computing resources needed and the energy levels present at the IoT nodes. Certificate-less public key algorithms are also being applied to IoT. However, initial attempts at the design of certificate-less mechanism may not be suitable for IoT (Shi et al., 2014). Mahalle et al. (2014) have adapted a group based authentication methodology instead of individually authenticating each and every IoT device. This brings another option for system designers to consider innovatively tackling the issue of scalability.

6.4. *Standardization efforts*

One of the biggest challenges in IoT is to support heterogeneity, and be secure at the same time (Sheng et al., 2013). Currently, many types of devices and standards co-exist in one application. All of them provide information to the back-end systems or communicate with other devices using traditional security schemes. However, these devices cannot directly communicate with each other due to interfacing issues. Thus, a common gateway is used to coordinate all autonomic decisions amongst the constituents. This gateway should have an interface that can understand the proprietary security protocol used by a specific device and translate it in common language such as IP. Gateway plays an important role that provides interface between heterogeneous devices to the Internet, and interfacing the security requirements. In the context of autonomic computing, a gateway becomes the ideal candidate to represent autonomic manager.

IP is the common communication language used by almost all devices in the Internet and forms the basis of IoT communication. Based on that, internet experts suggested a new stripped-down version of IP for use in WSNs. Schemes of Low power Wireless Personal Area Network (6LoWPAN) (Shelby and Bormann, 2011) and Routing Over Low power and Lossy networks (ROLL) (Watteyne et al., 2011), which use IP for low power devices, have been formed under Internet Engineering Task Force (IETF). These open standards have defined a number of schemes that focus on secure communication and failsafe routing. With the use of 6LoWPAN, wireless sensor nodes that are previously not addressable are now reachable through the Internet. However, the continued implementation of the complete IPsec stack to protect mobile devices, the inability to implement individual local firewalls as well as the implementation of TLS is something to be looked into. Similarly, the limitation of implementation of TLS has given rise to Datagram TLS (DTLS) which is being preferred over TCP based TLS (Hartke, 2014). However, being based on UDP, implementation of DTLS needs to ensure reliable packet delivery during the initial handshake process.

Few other standards are recommended to be used on various low-power devices for higher layers. Message Queuing Telemetry Transport (MQTT) (Locke, 2011) is an open message protocol for M2M communications that enables the transfer of telemetry-style data. Other existing standards are Zigbee (Baronti et al., 2007), Wireless HART (Song et al., 2008), and Low Power WIFI (Dobkin and Aboussouan, 2009), which include fundamental security mechanisms for communication. Any additional autonomic security solutions will have to be dependent on these messaging techniques to allow for the transfer of control data.

Data from IoT devices can be sent to the autonomic manager to be processed or the managed device itself can make appropriate decision based on certain rules. In autonomic IoT, end devices do not only push data to a central location, they also have some self-* properties for them to act based on the environment they are working on. In this event, communication standards have to be compatible in dynamic environments. The data produced by IoT end devices has to be transformed into information so that it can have meaning. Based on input from few sources and by using semantic technology, the information can then be transformed into knowledge that is useful for making decision in some scenarios.

Internet engineers have also proposed new IETF working groups specifically for IoT communication. Two important new schemes under these working groups are DTLS In Constrained Environments (DICE) (Hartke and Bergmann, 2014). In addition, a new application layer protocol has been introduced to be used to translate HTTP for low-power devices. This standard, termed as Constrained Application Protocol (CoAP) is being widely used to replace HTTP as the higher level protocol (Shelby et al., 2013). CoAP is customized for use in IoT, and utilizes specific features from HTTP for the same. The usage of HTTP security protocol (HTTPS) is supported but limited. Few other standards are being proposed for this such as the IETF-constrained RESTful environment (CORE) scheme (Shelby, 2012). Open source IoT (OSIOT) (Koster and McNeil, 2013) provides an IoT toolkit that enables interoperability across networks by introducing methods for seamless service integration and secure communication, for example, by using RESTful APIs (Fielding, 2000). An autonomic system requires communication between the components in order to coordinate the decisions appropriately. DICE is still in the initial phase and work is being done to include CoAP group communication, as well as ensure source authentication (Kumar, 2014). Readers are recommended to go through the work by Sheng et al. (2013) for a survey of current IETF standardization attempts in more detail.

6.4.1. Additional remarks

On a final note, none of the above mentioned security schemes have been evaluated in terms of the complexity level, computational resources required and energy consumption levels at the IoT node. These serve as design level roadblocks, and a fresh look into the design process of such security approaches is needed. For example, security solutions that involve a low level physical human intervention are encouraged rather than relying totally on autonomic software solutions. Complete autonomic security is still a research dream and currently autonomy exists in discrete, independent parts. Partial autonomy does exist, and the future research should strive to build vertically towards the goal of complete, yet robust autonomic secure system.

Acknowledgments

This work was sponsored by the Ministry of Higher Education Malaysia (MOHE) under Exploratory Research Grant Scheme (ERGS) Number ERGS13-023-0055. The authors are highly thankful to the reviewers for their comments and suggestions.

References

Abbas S, Merabti M, Llewellyn-Jones D, Kifayat K. Lightweight Sybil attack detection in MANETs. IEEE Syst J 2013;7(2):236–48. http://dx.doi.org/10.1109/JSYST.2012.2221912.

Altolini D, Lakkundi V, Bui N, Tapparello C, Rossi M. Low power link layer security for IoT: implementation and performance analysis. In: Proceedings of the 9th international wireless communications and mobile computing conference, IWCMC 2013. Sardinia (Italy): Institute of Electrical and Electronics Engineers; July 2013. p. 919–25.

Amin M. Toward self-healing energy infrastructure systems. IEEE Comput Appl Power 2002;14(1):20–8. http://dx.doi.org/10.1109/67.893351.

Arkko J, Devarapalli V, Dupont F. Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents. Network Working Group [Internet]. Internet Engineering Task Force; 2004 [cited 2014 Sep 1]. Available from ⟨http://tools.ietf.org/rfc/rfc3776.txt⟩.

Ashraf QM, Habaebi MH, Chebil J. SIHAT: simplifying interfaces in health-nets for achieving telemetry. In: Adnan Hye Qazi Muhammad, editor. Handbook on the emerging trends in scientific research. Pakistan: Pak Publishing Group; 2014. p. 207–17.

Ashraf QM, Habaebi MH, Sinniah GR, Ahmed MM, Khan S, Hameed S. Autonomic protocol and architecture for devices in Internet of Things. In: Proceedings of IEEE innovative smart grid technologies—Asia, ISGT Asia 2014. Kuala Lumpur (Malaysia): Institute of Electrical and Electronics Engineers; 2014b. p. 737–42.

Ashraf QM, Habaebi MH, Sinniah GR, Chebil J. Broadcast based registration technique for heterogenous nodes in the IoT. In: Proceedings engineering & technology, PET 2014. Sousse (Tunisia): International Publisher & C.O; 2014c. p. 45–50.

Babaoglu O, Jelasity M, Montresor A, Fetzer C, Leonardi S, van Moorsel A. et al. The self-star vision. Ozalp Babaoglu, Márk Jelasity, Alberto Montresor, Christof Fetzer, Stefano Leonardi, Aad van Moorsel, Maarten van Steen (Eds.) In: Self-star properties in complex information systems. Berlin Heidelberg: Springer, 10.1007/11428589_1; 2005. p. 1–20.

Babar S, Stango A, Prasad N, Sen J, Prasad R. Proposed embedded security framework for Internet of Things (IoT). In: Proceedings of 2nd international conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology, wireless VITAE 2011. Chennai (India): Institute of Electrical and Electronics Engineers, 10.1109/WIRELESSVITAE.2011.5940923; 2011. p. 1–5.

Baronti P, Pillai P, Chook VWC, Chessa S, Gotta A, Hu YF. Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards. Comput Commun 2007;30(7):1655–95. http://dx.doi.org/10.1016/j.comcom.2006.12.020.

Battat N, Seba H, Kheddouci H. Monitoring in mobile ad hoc networks: a survey. Comput Netw 2014;69:82–100. http://dx.doi.org/10.1016/j.comnet.2014.04.013.

Bhargav-Spantzel A, Squicciarini AC, Bertino E. Trust negotiation in identity management. IEEE Secur Priv 2007;5(2):55–63. http://dx.doi.org/10.1109/MSP.2007.46.

Bysani LK, Turuk AK. A survey on selective forwarding attack in wireless sensor networks. In: Proceedings of international conference on devices and communications, ICDeCom 2011. Mesra (India): Institute of Electrical and Electronics Engineers; 2011. p. 1–5.

Cai Y, Pelechrinis K, Wang X, Krishnamurthy P, Mo Y. Joint reactive jammer detection and localization in an enterprise WiFi network. Comput Netw 2013;57(18):3799–811. http://dx.doi.org/10.1016/j.comnet.2013.09.004.

Canzanese R, Kam M, Mancoridis S. Toward an automatic, havioral malware classification system. In: Proceedings of the 7th international conference on self-adaptive and self-organizing systems, SASO 2013. Philadelphia (United States of America): Institute of Electrical and Electronics Engineers, 10.1109/SASO.2013.8; 2013. p. 111–20.

Carmilema J, Medrano MA, Flores D. Detection and mitigation of MITM attacks in storage cloud infrastructures. Rev Digit Cient Technol 2012;1:26–30.

Chaqfeh MA, Mohamed N. Challenges in middleware solutions for the internet of things. In: Proceedings of international conference on collaboration technologies and systems, CTS 2012. Denver (United States of America): Institute of Electical and Electronics Engineers, doi:10.1109/CTS.2012.6261022; 2012. p. 21–6.

Chen D, Chang G, Jin L, Ren X, Li J, Li F. A novel secure architecture for the Internet of Things. In: Proceedings of fifth international conference on genetic and evolutionary computing, ICGEC 2011. Xiamen (China): Institute of Electrical and Electronics Engineers, doi:10.1109/ICGEC.2011.77; 2011. p. 311–14.

Chen TM, Nguyen N. Authentication and privacy. In: Encyclopedia of wireless and mobile communications: Taylor & Francis, doi:10.1081/E-EWMC-120043167; 2008.

Choi BG, Cho EJ, Kim JH, Hong CS, Kim JH. A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In: Proceedings of the international conference on information networking, ICOIN 2009. Chiang Mai(Thailand): Institute of Electrical and Electronics Engineers; 2009. p. 1–5.

Coen-Porisini A, Colombo P, Sicari S. Privacy aware systems: from models to patterns. In: Haralambos Mouratidis, editor. Software Engineering for Secure Systems: Industrial and Research Perspectives. UK: IGI Global, University of East London; 2010. p. 232–59. http://dx.doi.org/10.4018/978-1-61520-837-1.ch009.

Corson S, Macker J. Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations [Internet]. Internet Engineering Task Force; 1999 [cited 2014 Sep 14]. Available from ⟨http://tools.ietf.org/html/rfc2501⟩.

Dai HN, Wang Q, Li D, Wong RCW. On eavesdropping attacks in wireless sensor networks with directional antennas. Int J Distrib Sens Netw 2013;2013:1–13. http://dx.doi.org/10.1155/2013/760834.

Delfs H, Knebl H. Symmetric-key encryption. In: Introduction to cryptography. Berlin: Springer; 2007. p. 11–31.

Deng H, Sun X, Wang B, Cao Y. Selective forwarding attack detection using watermark in WSNs. In: Proceedings of ISECS international colloquium on computing, communication, control and management, CCCM 2009. Sanya (China): Institute of Electrical and Electronics Engineers, 10.1109/CCCM.2009.5268016 ; 2009. p. 109–13.

Di Pietro R, Ma D, Soriente C, Tsudik G. POSH: Proactive co-operative self-healing in unattended wireless sensor networks. In: Proceedings of IEEE symposium on reliable distributed system, SRDS 2008. Naples(Italy): Institute of Electrical and Electronics Engineers, 10.1109/SRDS.2008.23; 2008. p. 185–94.

Di Pietro R, Mancini LV, Soriente C, Spognardi A, Tsudik G. Data security in unattended wireless sensor networks. IEEE Trans Comput 2009;58(11):1500–11. http://dx.doi.org/10.1109/TC.2009.109.

Dobkin DM, Aboussouan B. Low power Wi-Fi™(IEEE802.11) for IPsmart objects. Los Gatos (CA): Gainspan Corporation; 2009.

Dutta R, Dong Wu Y, Mukhopadhyay S. Constant storage self-healing key distribution with revocation in wireless sensor network. In: Proceedings of IEEE international conference on communications, ICC 2007. Glasgow(Scotland):

Institute of Electrical and Electronics Engineers, 10.1109/ICC.2007.223; 2007. 1323–28.

Feng D, Jiang C, Lim G, Cimini Jr LJ, Feng G, Li GY. A survey of energy-efficient wireless communications. IEEE Commun Surv Tutor 2013;15(1):167–78. http://dx.doi.org/10.1109/SURV.2012.020212.00049.

Fielding RT. (PhD thesis). Representational State Transfer (REST). Irvine: University of California; 2000.

Fischer K, Gesner J. Security architecture elements for IoT enabled automation networks. In: Proceedings of 17th international conference on emerging technologies & factory automation, ETFA 2012. Krakow (Poland): Institute of Electrical and Electronics Engineers, 10.1109/ETFA.2012.6489651; 2012. 1–8.

Ganta SR, Kasiviswanathan SP, Smith A. Composition attacks and auxiliary information in data privacy. In: Proceedings of the 14th ACM international conference on knowledge discover and data mining, SIGKDD 2002. Las Vegas (United States of America): Association for Computing Machinery, 10.1145/1401890.1401926; 2008. p. 265–73.

Ghosh D, Sharman R, Raghav Rao H, Upadhyaya S. Self-healing systems-survey and synthesis. Decis Support Syst 2007;42(4):2164–85. http://dx.doi.org/10.1016/j.dss.2006.06.011.

Gluhak A, Krco S, Nati M, Pfisterer D, Mitton N, Razafindralambo T. A survey on facilities for experimental internet of things research. IEEE Commun Mag 2011;49(11):58–67. http://dx.doi.org/10.1109/MCOM.2011.6069710.

Grover K, Lim A. A survey of broadcast authentication schemes for wireless sensor networks. Ad Hoc Netw 2015;24(A):288–316. http://dx.doi.org/10.1016/j.adhoc.2014.06.008.

Gu L, Wang J, Sun B. Trust management mechanism for Internet of Things. Ch Commun 2014;11(2):148–56. http://dx.doi.org/10.1109/CC.2014.6821746.

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(7):1645–60. http://dx.doi.org/10.1016/j.future.2013.01.010.

Gui C, Mohapatra P. SHORT: self-healing and optimizing routing techniques for mobile ad hoc networks. In: Proceedings of the 4th ACM international symposium on mobile ad hoc networking & computing, MobiHoc 2003. Annapolis(United States of America): Association for Computing Machinery, 10.1145/778415.778448; 2003. 279–90.

Habaebi MH, Ashraf QM. System and method for detecting jammers in a wireless network and optimizing operation of the network. Malaysian Patent Pending PI 2014002288; 2014 August.

Hammer S, Wißner M, André E. Trust-based decision-making for energy-aware device management. In: Vania Dimitrova, Tsvi Kuflik, David Chin, Francesco Ricci, Peter Dolog, Geert-Jan Houben, editors. User modeling, adaptation, and personalization. Switzerland: Springer International Publishing; 2014. p. 326–37. http://dx.doi.org/10.1007/978-3-319-08786-3_29.

Han S, Tian B, He M, Chang E. Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks. IEEE Trans Wirel Commun 2009;8(4):1876–87. http://dx.doi.org/10.1109/TWC.2009.080046.

Hartke K. Practical issues with datagram transport layer security in constrained environments [Internet]. Internet Engineering Task Force; 2014 [cited 2014 Jul 14]. Available from: 〈http://www.ietf.org/archive/id/draft-hartke-dice-practical-issues-01.txt〉.

Hartke K, Bergmann O. DTLS In constrained environments (DICE) [Internet]. Internet Engineering Task Force; 2013 [cited 2014 Sep 10]. Available from: 〈http://www.ietf.org/proceedings/83/slides/slides-83-lwig-2.pdf〉.

He D, Chen C, Chan S, Bu J, Vasilakos AV. ReTrust: attack-resistant and lightweight trust management for medical sensor networks. IEEE Trans Inf Technol Biomed 2012;16(4):623–32. http://dx.doi.org/10.1109/TITB.2012.2194788.

Henrici D, Müller P. Tackling security and privacy issues in radio frequency identification devices. In: Alois Ferscha, Friedemann Mattern, editors. Pervasive computing. Springer: Berlin Heidelberg; 2004. p. 219–24. http://dx.doi.org/10.1007/978-3-540-24646-6_16.

Howitt I, Gutierrez JA. IEEE 802.15.4 low rate—wireless personal area network coexistence issues. In: Proceedings of IEEE wireless communications and networking, WCNC 2003. New Orleans(USA): Institute of Electrical and Electronics Engineers, 10.1109/WCNC.2003.1200605; 2003. p. 1481–86.

Huebscher MC, McCann JA. A survey of autonomic computing-degrees, models, and applications. ACM Comput Surv 2008;40(3):2–28. http://dx.doi.org/10.1145/1380584.1380585.

Iera A, Floerkemeier C, Mitsugi J, Morabito G. Internet of Things. IEEE Wirel Commun 2010;17(6):8–9. http://dx.doi.org/10.1109/MWC.2010.5675772.

Jänig W. Autonomic nervous system. In: Robert F. Schmidt, Gerhrad Thews, editors. Human physiology. Springer: Berlin Heidelberg; 1989. p. 333–70.

Juels A. Minimalist cryptography for low-cost RFID tags. In: Carlo Blundo, Stelvio Cimato, editors. Security in communication networks. Berlin Heidelberg: Springer; 2005. p. 149–64. http://dx.doi.org/10.1007/978-3-540-30598-9_11.

Juels A, Rivest LR, Szydlo M. The blocker tag: selective blocking of RFID tags for consumer privacy. In: Proceedings of 10th ACM conference on computer and communication security, CCS 2003. Philadelphia(United States of America): Association for Computing Machinery, 10.1145/948109.948126; 2003. 103–11.

Kalloniatis C, Kavakli E, Gritzalis S. Addressing privacy requirements in system design: the pris method. Requir Eng 2008;13(3):241–55. http://dx.doi.org/10.1007/s00766-008-0067-3.

Kang T, Li X, Yu C, Kim J. A survey of security mechanisms with direct sequence spread spectrum signals. J Comput Sci Eng 2013;7(3):187–97. http://dx.doi.org/10.5626/JCSE.2013.7.3.187.

Kausar F, Hussain S, Park JH, Masood A. Secure group communicaiton with self-healing and rekeying in wireless sensor networks. In: Mobile ad-hoc and sensor networks. Berlin Heidelberg: Springer, 10.1007/978-3-540-77024-4_67; 2007. p. 737–48.

Kephart JO, Chess DM. The vision of autonomic computing. Computer 2003;36(1):41–50. http://dx.doi.org/10.1109/MC.2003.1160055.

Kim KH, Shin KG. Self-healing multi-radio wireless mesh networks. In: Proceedings of the 13th Annual ACM international conference on mobile computing and networking, MobiCom 2007. Montreal(Canada): Association for Computing Machinery, 10.1145/1287853.1287896; 2007. 326–29.

Kim YK, Lee H, Cho K, Lee DH. CADE: Cumulative acknowledgement based detection of selective forwarding attacks in wireless sensor networks. In: Proceedings of third international conference on convergenece and hybrid information technology, ICCIT 2008. Busan(South Korea): Institute of Electrical and Electronics Engineers, 10.1109/ICCIT.2008.271; 2008. 416–22.

Koehler J, Giblin D, Gantenbein D, Hauser R. On autonomic computing architectures. Ruschlikon (Switzerland): IBM Research Zurich Research Laboratory; 2003.

Koh JY, Ming JTC, Niyato D. Rate limiting client puzzle schemes for denial-of-service mitigation. In: Proceedings of IEEE wireless communications and networking conference, WCNC 2013. Shanghai(China): Institute of Electrical and Electronics Engineers, 10.1109/WCNC.2013.6554845; 2013. p. 1848–53.

Kothmayr T, Schmitt C, Hu W, Brünig M, Carle G. DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Netw 2013;11(8):2710–23. http://dx.doi.org/10.1016/j.adhoc.2013.05.003.

Krontiris I, Dimitriou T, Giannetsos T, Mpasoukos M. Intrusion detection of sinkhole attacks in wireless sensor networks. In: Miroslaw Kutylowski, Jacek Cichon, Przemyslaw Kubiak, editors. Algorithmic aspects of wireless sensor networks. Berlin Heidelberg: Springer; 2008. p. 150–61 http://dx.doi.org/10.1007/978-3-540-77871-4_14.

Kumar S. Group communication security for low-power and lossy networks (LLNs) [Internet]. Internet Engineering Task Force; 2014 [cited 2014 Sep 7]. Available from: 〈https://datatracker.ietf.org/doc/draft-kumar-dice-groupcomm-security/〉.

Kushalnagar N, Montenegro G, Schumacher C. IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals [Internet]. Internet Engineering Task Force; 2007 [cited 2014 Aug 2]. Available from 〈http://tools.ietf.org/html/rfc4919〉.

Lalanda P, McCann JA, Diaconescu A. Future of autonomic computing and conclusions. In: Philippe Lalanda, Julie A McCann, Ada Diaconescu, editors. Autonomic computing: principles, design and implementation. London: Springer; 2013. p. 263–78. http://dx.doi.org/10.1007/978-1-4471-5007-7_10.

Lee JY, Lin WC, Huang YH. A lightweight authentication protocol for the Internet of Things. In: Proceedings of the international symposium on next-generation electronics, ISNE 2014. Kwei-Shan (Taiwan): Institute of Electrical and Electronic Engineers, 10.1109/ISNE.2014.6839375; 2014. 1–2.

Lin X. LSR: mitigating zero-day Sybil vulnerability in privacy-preserving vehicular peer-to-peer networks. IEEE J Sel Areas Commun 2013;31(9):237–46. http://dx.doi.org/10.1109/JSAC.2013.SUP.0513021.

Lioudakis GV, Koutsoloukas EA, Dellas N, Kapellaki S, Prezerakos GN, Kaklamani DI et al. A proxy for privacy: the discreet box. In: Proceedings of the international conference on computer as a tool, EUROCON 2008. Warsaw(Poland): Institute of Electrical and Electronics Engineers, 10.1109/EURCON.2007.4400521; 2007. 966–73.

Liu J, Xiao Y, Chen CLP. Authenctication and access control in the Internet of Things. In: Lluís Fàbrega, Pere Vilà, Davide Careglio, Dimitri Papadimitriou, editors. Proceedings of 32nd international conference on distributed computing systems workshops, ICDCSW. Macau(China): Institute of Electrical and Electronics Engineers; 2012. p. 588–92. http://dx.doi.org/10.1109/ICDCSW.2012.23.

Liu W, Keranidis S, Mehari M, Vanhie-Van Gerwen J, Bouckaert S, Yaron O, Moerman I. Various detection techniques and platforms for monitoring interference condition in a wireless testbed. In: Measurement methodology and tools. Berlin Heidelberg: Springer, 10.1007/978-3-642-41296-7_4; 2013. p. 43–60.

Liu Z, Liu H, Xu W, Chen Y. Wireless jamming localization by exploiting nodes' hearing ranges. Rajmohan Rajaraman, Thoma, s Moscibroda, Adam Dunkels, Anna Scaglione (Eds.) In: Distributed computing in sensor systems. Berlin Heidelberg: Springer, 10.1007/978-3-642-13651-1_25; 2010. p. 348–61.

Locke D. MQTT V3.1 Protocol Specification [Internet]. International Business Machines Corporation (IBM); 2011. [cited 2014 Aug 14] Available from: 〈http://www.ibm.com/developerworks/library/ws-mqtt/〉.

Loveland S, Hulten GJ, Haber EJ, Scarrow JL. Online risk mitigation. United States Patent US 8429743 B2; 2008 December 23.

Mahalle PN, Prasad NR, Prasad R. Threshold cryptography-based group authentication (TCGA) scheme for the Internet of Things. In: Proceedings of the 4th international conference on wireless communicatons, vehicular technology, information theory and aerospace & electronic systems, VITAE 2014. Aalborg (Denmark): Institute of Electrical and Electronics Engineers, 10.1109/VITAE.2014.6934425; 2014. 1–5.

Manzo M, Roosta T, Sastry S. Time synchronisation attacks in sensor networks. In: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks, SASN 2005. Alexandria(United States of America): Association for Computing Machinery, 10.1145/1102219.1102238; 2005. 107–16.

McCusker K, O'Connor NE. Low energy symmetric key distribution in wireless sensor networks. IEEE Trans Depend Secur Comput 2011;8(3):363–76. http://dx.doi.org/10.1109/TDSC.2010.73.

Millett LI, Holden SH. Authentication and its privacy effects. IEEE Internet Comput 2003;7(6):54–8. http://dx.doi.org/10.1109/MIC.2003.1250584.

Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: vision, applications and research challenges. Ad Hoc Netw 2012;10(7):1497–516. http://dx.doi.org/10.1016/j.adhoc.2012.02.016.

Mobahat H. Authentication and lightweight cryptography in low cost RFID. In: Proceedings of 2nd international conference on software technology and engineering, ICSTE 2010. San Juan(United States of America): Institute of Electrical and Electronics Engineers, 10.1109/ICSTE.2010.5608776; 2010. 123–9.

Mohebi A, Scott S. A survey on mitigation methods to black hole attack on AODV routing protocol. Netw Complex Syst 2013;3(9):30–6.

Ning H, Liu H, Yang LT. Cyber-entity security in the Internet of Things. Computer 2013;46(4):46–53. http://dx.doi.org/10.1109/MC.2013.74.

Ohkubo M, Suzuki K, Kinoshita S, 2004. Efficient hash-chain based RFID privacy protection scheme. In: Proceedings of international conference on ubiquitous computing, Ubicomp 2004.

O'Neill M. The Internet of Things: do more devices mean more risks? Comput Fraud Secur 2014;2014(1):16–7. http://dx.doi.org/10.1016/S1361-3723(14)70008-9.

Pan J, Paul S, Jain R. A survey of the research on future Internet architectures. IEEE Commun Mag 2011;49(7):26–36. http://dx.doi.org/10.1109/MCOM.2011.5936152.

Pandarinath P. Secure localization with defense against selective forwarding attacks in wireless sensor networks. In: Proceedings of 3rd international conference on electronics computer technology, ICECT 2011. Kanyakumari(India): Institute of Electrical and Electronics Engineers, 10.1109/ICECTECH.2011.5941968; 2011. 112–7.

Pawar S, El Rouayheb S, Ramchandran K. Securing dynamic distributed storage systems against eavesdropping and adversarial attacks. IEEE Trans Inf Theory 2011;57(11):6734–53. http://dx.doi.org/10.1109/TIT.2011.2162191.

Petrov V, Edelev S, Komar M, Koucheryavy Y. Towards the era of wireless keys: how the IoT can change authentication paradigm. In: Proceedings of IEEE world forum on Internet of Things, WF-IoT 2014. Seoul (South Korea): Institute of Electrical and Electronics Engineers, 10.1109/WF-IoT.2014.6803116; 2014. 51–6.

Ping Y, Yafei H, Yiping Z, Shiyong Z, Zhoulin D. Flooding attack and defence in ad hoc networks. IEEE J Syst Eng Electron 2006;17(2):410–6. http://dx.doi.org/10.1016/S1004-4132(06)60070-4.

Poor R, Bowman C, Auburn CB. Self-healing networks. ACM Wirel Queue 2003;1(3):52–9. http://dx.doi.org/10.1145/846057.864027.

Qu G, Hariri S, Jangiti S, Rudraraju J, Oh S, Fayssal S et al. Online monitoring and analysis for self-protection against network attacks. In: Proceedings of international conference on autonomic computing: Institute of Electrical and Electronics Engineers, 10.1109/ICAC.2004.1301398; 2004. 324–5.

Rabbachin A, Conti A, Win MZ. Intentional network interference for denial of wireless eavesdropping. In: Proceedings of IEEE global telecommunications conference, GLOBECOM 2011. Houston (United States of America): Institute of Electrical and Electronics Engineers, 10.1109/GLOCOM.2011.6134361; 2011. 1–6.

Ren W, Yu L, Ma L, Ren Y. How to authenticate a device? Formal authentication models for M2M communications defending against ghost compromising attack Int J Distrib Sens Netw 2013;2013:1–9.

Riahi A, Challal Y, Natalizio E, Chtourou Z, Bouabdallah A. A systemic approach for IoT security. In: Proceedings of international conference on distributed computing in sensor systems, DCOSS 2013. Cambridge(United States of America): Institute of Electrical and Electronics Engineers, 10.1109/DCOSS.2013.78; 2013. 351–5.

Roman R, Najera P, Lopez J. Securing the Internet of Things. Computer 2011;44(9):51–8. http://dx.doi.org/10.1109/MC.2011.291.

Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Comput Netw 2013(10):2266–79. http://dx.doi.org/10.1016/j.comnet.2012.12.018.

Schaffer P, Farkas K, Horváth Á, Holczer T, Buttyán L. Secure and reliable clustering in wireless sensor networks: a critical survey. Comput Netw 2012;56(11):2726–41. http://dx.doi.org/10.1016/j.comnet.2012.03.021.

Sehgal A, Perelman V, Kuryla S, Schonwalder J. Management of resource constrained devices in the Internet of Things. IEEE Commun Mag 2012;50(12):144–9. http://dx.doi.org/10.1109/MCOM.2012.6384464.

Sexton M, Smith E, Eydt B. Wireless security. In: Wiley Handbook of Science and Technology for Homeland Security. Wiley Online Library; 2009. p. 1-15. doi: 0.1002/9780470087923.hhs453.

Shafiei H, Khonsari A, Derakhshi H, Mousavi P. Detection and mitigation of sinkhole attacks in wireless sensor networks. J Comput Syst Sci 2014;80(3):644–53. http://dx.doi.org/10.1016/j.jcss.2013.06.016.

Shelby Z. Constrained RESTful environments (CoRE) link format [Internet]. Internet Engineering Task Force; 2012 [cited 2014 Aug 1]. Available from: ⟨http://tools.ietf.org/html/rfc6690⟩.

Shelby Z, Bormann C. 6LoWPAN: the wireless embedded internet. . John Wiley & Sons; 2011.

Shelby Z, Hartke K, Bormann C. Constrained application protocol (CoAp) [Internet]. Internet Engineering Tas Force; 2013 [cited 2014 Sep 5]. Available from: ⟨http://tools.ietf.org/html/draft-ietf-core-coap-18⟩.

Sheng Z, Yang S, Yu Y, Vasilakos AV, McCann JA, Leung KK. A survey on the IETF protocol suite for the Internet of Things: standards, challenges, and opportunities. IEEE Wirel Commun 2013;20(6):91–8. http://dx.doi.org/10.1109/MWC.2013.6704479.

Shi W, Kumar N, Gong P, Chilamkurti N, Chang H. On the security of a certificateless online/offline signcryption for Internet of Things. Peer-to-Peer Netw Appl 2014:1–5. http://dx.doi.org/10.1007/s12083-014-0249-3.

Shila DM, Anjali T. Defending selective forwarding attacks in WMNs. In: Proceedings of IEEE international conference on electro/information technology, EIT 2008. Ames(United States of America): Institute of Electrical and Electronics Engineers, 10.1109/EIT.2008.4554274; 2008. 96–101.

Shoreh M, Hosseinianfar H, Akhoundi F, Yazdian E, Farhang M, Salehi J. Design and implementation of spectrally-encoded spread-time CDMA transceiver. IEEE Commun Lett 2014;18(5):741–4. http://dx.doi.org/10.1109/LCOMM.2014.033114.132471.

Singh VP, Jain S, Singhai J. Hello flood attack and its countermeasures in wireless sensor networks. Int J Comput Sci 2010;7(11):23–7.

Song J, Han S, Mok AK, Chen Deji, Lucas M, Nixon M. WirelessHART: applying wireless technology in real-time industrial process control. In: Proceedings of real-time and embedded technology and applications symposium, RTAS 2008. St. Louis(United States of America): Institute of Electrical and Electronic Engineers, 10.1109/RTAS.2008.15; 2008. 377–86.

Sweeney L. Achieving k-anonymity privacy protection using generalisation and suppression. Int J Uncertain Fuzziness Knowl-Based Syst 2002a;10(5):571–88. http://dx.doi.org/10.1142/S021848850200165X.

Sweeney L. k-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness Knowl-Based Syst 2002b;10(5):557–70.

Ukil A, Sen J, Koilakonda S. Embedded security for Internet of Things. In: Proceedings of 2nd national conference on emerging trends and applications in computer science, NCETACS 2011. Shillong(India): Institute of Electrical and Electronics Engineers, 10.1109/NCETACS.2011.5751382; 2011. 1–6.

Vassev E, Hinchey M. The ASSL formalism for real-time autonomic systems. In: Teresa-M Higuera-Toledano, Uwe Brinkschulte, Achim Rettberg, editors. Self-organization in embedded real-time systems. New York: Springer; 2013. p. 151–77. http://dx.doi.org/10.1007/978-1-4614-1969-3_8.

Vidalis S, Angelopoulou O. Assessing identity theft in the Internet of Things. In: Proceedings of IT convergence practice, INPRA; 2014. p. 14–20.

Vlajic N, Moniz N. Self-healing wireless sensor networks: results that may surpirse. In: Proceedings of IEEE globecom workshops. Washington (United States of America): Institute of Electrical and Electronics Engineers, 10.1109/GLOCOMW.2007.4437830; 2007. 1–7.

Vucinic M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R. OSCAR: Object security architecture for the Internet of Things [Internet]. arXiv preprint arXiv:1404.7799; 2014 [cited 2014 Nov 2]. Available from: ⟨http://arxiv.org/abs/1404.7799⟩.

Wang Y, Li M, Zhang Q. Efficient algorithms for p-self-protection problem in static wireless sensor networks. IEEE Trans Parallel Distrib Syst 2008;19(10):1426–38. http://dx.doi.org/10.1109/TPDS.2008.13.

Wang Y, Nakao A, Vasilakos AV, Ma J. P2P soft security: on evolutionary dynamics of P2P incentive mechanism. Comput Commun 2011;34(3):241–9. http://dx.doi.org/10.1016/j.comcom.2010.01.021.

Wasilewski K, Branch JW, Lisee M, Szymanski BK. Self-healing routing: a study in efficiency and resiliency of data delivery in wireless sensor networks. In: Proceedings of unattended ground, sea, and air sensor technologies and applications IX. Florida(United States of America):SPIE, 10.1117/12.723515; 2007.

Watteyne T, Molinaro A, Richichi MG, Dohler M. From MANET to IETF ROLL Standardization: a paradigm shift in WSN routing protocols. IEEE Commun Surv Tutor 2011;13(4):688–707. http://dx.doi.org/10.1109/SURV.2011.082710.00092.

Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, et al. Security and privacy for storage and computation in cloud computing. Inf Sci 2014;258:371–86. http://dx.doi.org/10.1016/j.ins.2013.04.028.

Wei L, Zhu H, Cao Z, Jia W, Vasilakos AV. SecCloud: bridging secure storage and computation in cloud. In: Proceedings of IEEE 30th International conference on distributed computing systems wokshops, ICDCSW 2010. Genova(Italy): Institute of Electrical and Electronics Engineers, 10.1109/ICDCSW.2010.36; 2010. 52–61.

Weis SA, Sarma SE, Rivest RL, Engels DW. Security and privacy aspects of low-cost radio frequency identification systems. In: Dieter Hutter, Günter Müller, Werner Stephan, Markus Ullmann, editors. Security in pervasive computing. Berlin Heidelberg: Springer; 2004. p. 201–12. http://dx.doi.org/10.1007/978-3-540-39881-3_18.

Wood A, Stankovic JA, Zhou G. DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In: Proceedings of 4th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks, SECON '07. San Diego(United States of America): Institute of Electrical and Electronics Engineers, doi:10.1109/SAHCN.2007.4292818; 2007. 60–9.

Wrightson T. Principle 9: CIA triad. In: Wireless network security: a beginner's guide. 1st Edition. McGraw-Hill; 2012.

Xiang M, Bai Q, Liu W. Trust-based adaptive routing for smart grid systems. J Inf Process 2014;22(2):210–8. http://dx.doi.org/10.2197/ipsjjip.22.210.

Xiao S, Gong W, Towsley D. Secure wireless communication with dynamic secrets. In: Proceedings of INFOCOM 2010. San Diego(United States of America): Institute of Electrical and Electronics Engineers, doi:10.1109/INFCOM.2010.5461974; 2010. 1–9.

Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. J Netw Comput Appl 2014;42:120–34. http://dx.doi.org/10.1016/j.jnca.2014.01.014.

Yu H, Gibbons PB, Kaminsky M, Xiao F. SybilLimit: a near-optimal social network defense against Sybil attacks. In: Proceedings of symposium on security and privacy, SP 2008. Oakland(United States of America): Institute of Electrical and Electronics Engineers, doi: 10.1109/SP.2008.13; 2008a. 3–17.

Yu H, Kaminsky M, Gibbons PB, Flaxman AD. SybilGuard: defending against Sybil attacks via social networks. IEEE/ACM Trans Netw 2008b;16(3):576–89. http://dx.doi.org/10.1109/TNET.2008.923723.

Zhang B, Zou Z, Liu M. Evaluation on security system of Internet of Things based on fuzzy-AHP method. In: Proceedings of the international conference on e-business and e-government, ICEE 2011. Shanghai (China): Institute of Electrical and Electronics Engineers, 10.1109/ICEBEG.2011.5881939; 2011. 1–5.

Zhang H, Arora A. GS3: scalable self-configuring and self-healing in wireless sensor networks. Comput Netw 2003;43(4):459–80. http://dx.doi.org/10.1016/S1389-1286(03)00354-2.

Zhao K, Ge L. A survey on the Internet of Things security. In: Proceedings of 9th international conference on computational intelligence and security, CIS 2013. Leshan (China): Institute of Electrical and Electronicss Engineers, 10.1109/CIS.2013.145; 2013. 663–7.

Zheng J, Simplot-Ryl D, Bisdikian C, Mouftah HT. The Internet of Things. IEEE Commun Mag 2011;49(11):30–1.

Zhou L, Chao HC. Multimedia traffic security architecture for the Internet of Things. IEEE Netw 2011;25(3):35–40. http://dx.doi.org/10.1109/MNET.2011.5772059.

Zhou T, Choudhury RR, Ning P, Chakrabarty K. P2DAP- Sybil attacks detection in vehicular ad hoc networks. IEEE J Sel Areas Commun 2011;29(3):582–94. http://dx.doi.org/10.1109/JSAC.2011.110308.