Computer Networks 148 (2019) 283–294

Contents lists available at ScienceDirect

Computer Networks

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

Current research on Internet of Things (IoT) security: A survey

Mardiana binti Mohamad Noor, Wan Haslina Hassan*

Computer Systems and Networks (CSN), Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Kuala Lumpur

ARTICLE INFO

Article history:
Received 6 August 2018
Revised 29 October 2018
Accepted 27 November 2018
Available online 1 December 2018

Keywords:
IoT security
Challenges
Current research
Simulation

ABSTRACT

The results of IoT failures can be severe, therefore, the study and research in security issues in the IoT is of extreme significance. The main objective of IoT security is to preserve privacy, confidentiality, ensure the security of the users, infrastructures, data, and devices of the IoT, and guarantee the availability of the services offered by an IoT ecosystem. Thus, research in IoT security has recently been gaining much momentum with the help of the available simulation tools, modellers, and computational and analysis platforms. This paper presents an analysis of recent research in IoT security from 2016 to 2018, its trends and open issues. The main contribution of this paper is to provide an overview of the current state of IoT security research, the relevant tools,IoT modellers and simulators.

1. Introduction

The Internet of Things (IoT) is envisioned to grow rapidly due the proliferation of communication technology, the availability of the devices, and computational systems. Hence, IoT security is an area of concern in order to safeguard the hardware and the networks in the IoT system. However, since the idea of networking appliances is still relatively new, security has not been considered in the production of these appliances.

Some examples of existing IoT systems are self-driving vehicles (SDV) for automated vehicular systems, microgrids for distributed energy resources systems, and Smart City Drones for surveillance systems. A microgrid system represents a good example of a cyber-physical system: it links all distributed energy resources (DER) together to provide a comprehensive energy solution for a local geographical region. However, a microgrid IoT system still relies on traditional Supervisory Control and Data Acquisition (SCADA). The integration of the physical and cyber domains actually increases the exposure to attacks: cyber attacks may target the SCADA supervisory control and paralyse the physical domain or the physical devices may be tampered or compromised, affecting the supervisory control system. On the other hand, the drone market is moving quickly to adopt automation techniques and can be integrated into fire fighting, police, smart city surveillance, and emergency response. As municipalities and citizens begin to rely on such a system, it will become critical to keep the system secure and reliable.

In recent years, it has been observed that academic research to address the privacy and security issues for IoT systems has attained positive developments. Currently, the techniques and security methods which have been proposed are essentially based on conventional network security methods. However, applying security mechanisms in an IoT system is more challenging than with a traditional network, due to the heterogeneity of the devices and protocols as well as the scale or the number of nodes in the system. The challenges in applying IoT security mitigation which are due to physical coupling, heterogeneity, resource constraints, privacy, the large scale, trust management and unpreparedness for security are extensively explained in [1].

The survey papers [2–6] evaluate the possible threats to IoT systems according to the layers and the available countermeasures. Kouicem et al. [7] stated that in recent years, there has been a lot of research to address issues such as key management, confidentiality, integrity, privacy, and policy enforcement for IoT systems, hence suggested traditional cryptography methods and new technologies such as Software Defined Network (SDN) and Blockchain to be implemented to solve current IoT security issues.

One of the key enablers of the rapid progress of academic IoT security research is the availability of a tool for IoT or sensor network simulation and modelling. A comprehensive list of the simulators used in current research is presented by Chernyshev et al. [8]. An open source network simulator, such as NS 3, is the most used simulator for IoT security research. However, since many new security protocols are being proposed, there is an urgent need for a security protocol evaluator, such as Automated Validation of Internet Security Protocols and Applications, AVISPA.

The present paper will survey the current development of IoT security research from 2016 to 2018. Challenges in applying security mechanisms in IoT and its attack vectors will also be evaluated. Simulators or IoT modellers that may be used by new researchers to further develop the IoT security field will be highlighted. The

* Correspondence author
E-mail addresses: mardiana22@graduate.utm.my (M.b. Mohamad Noor), wanhaslina.kl@utm.my (W.H. Hassan).

https://doi.org/10.1016/j.comnet.2018.11.025
1389-1286/

credibility of the published work surveyed here has been ensured by using the reputable Web of Knowledge search engine by using the keyword “IoT security simulation” . The contribution of this paper is highlighted by comparing several aspects of other surveys, such as techniques for IoT security mechanisms, simulation tools, and current research. Table 1 compares the present survey with the other surveys in IoT security published from 2017 to 2018. As compared to these other surveys, the present survey presents findings on the current IoT security mechanisms, including authentication, encryption, trust management, secure routing protocols, and new technologies applied to IoT security, along with the related tools and simulators involved in the research.

2. Background

The IoT architecture is based on a 3-tier/layer system which consists of a perception/hardware layer, a network/communication layer, and a layer of interfaces/services. The elements that make up an IoT system are hardware/devices, communication/messaging protocols, and interfaces/services.

Hardware, such as the sensors and actuators, comprises the most important elements in the IoT. The typical microprocessor which is used at the hardware layer is usually based on the ARM, MIPS or X86 architectures. Ideally, developers should also incorporate security hardware, which may include a cryptographic code processor or security chip.

For the hardware operating system, IoT devices typically use a Real Time Operating System (RTOS), which includes a microkernel, hardware abstraction layer, communication drivers, and capabilities such as process isolation, secure boots, and application sandbox. For the application software layer, there are custom applications, cryptographic protocols, and third party libraries and drivers.

In particular, hardware selection is critical for securing the IoT devices. The concerns regarding the IoT hardware are authentication capabilities, end-to-end traffic encryption, secure boot-loading process, the enforcement of digital signatures during firmware updates, and transparent transactions.

The next important component of an IoT system includes the communication and messaging protocols. A network of smart objects can communicate directly to the Cloud via a gateway, through cloud services such as Amazon Kinesis. However, the important concept of IoT is implementing a Wireless Sensor Network (WSN) as the main communication technology in the IoT. WSN has lightweight protocols for the devices to communicate with each other and with the gateway at the edge. Moreover, WSN supports dynamic communication, which is usually always based on the 802.15.4 standard. Among the IEEE protocols, 802.15.4 is for Low Rate WPANs, which suits the requirements for an IoT system. Some advantages of this protocol are its scalability and the fact that it can be self-maintained, uses little power, and has a low operational cost. However, Bluetooth, ZigBee, PLC, WiFi, 4G and 5G may also be chosen as the communication protocols, to suit the needs of the IoT processes.

Another important component in the IoT is the aggregator, which can be the gateway for an IoT architecture, such as a WiFi router. Gateways provide downstream connectivity to multiple “things” . The Cloud is another core element in an IoT system. Some popular Cloud Service Providers (CSPs) are Amazon Web Services, Microsoft Azure, Google Cloud Platform and IBM Cloud (to name a few) . The Cloud provides services for the IoT, including messaging, storage, data processing and analytics. In addition, new support features are being offered by CSPs which support Message Queuing Telemetry Transport (MQTT), which is usually used in machine to machine (M2M) communication, and Represential State Transfer (REST) communication protocols.

Table 1
IoT security survey from 2017 until 2018.

	Reference Publisher	[3] IEEE	[2] IEEE	[6] Elsevier	[5] Elsevier	[4] Elsevier	[1] Elsevier	[7] Elsevier	This survey
	Year	2017	2017	2017	2017	2018	2018	2018	2018
1.	***IoT simulation tools/platform***	No	No	No	No	Yes	No	No	Yes
2.	***Research in 2018***	No	No	No	No	No	Yes	Yes	Yes
3.	***Trend of the IoT security mitigation research***	No	No	Yes	Yes	No	No	Yes	Yes
4.	***Authentication***	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
5.	***Encryption***	Yes	No	No	Yes	No	Yes	Yes	Yes
6.	***Trust***	No	No	No	Yes	No	Yes	No	Yes
7.	***Secure routing protocol***	No	No	No	No	No	No	No	Yes
8.	***New Security Technology***	No	No	Yes	No	No	No	Yes	Yes

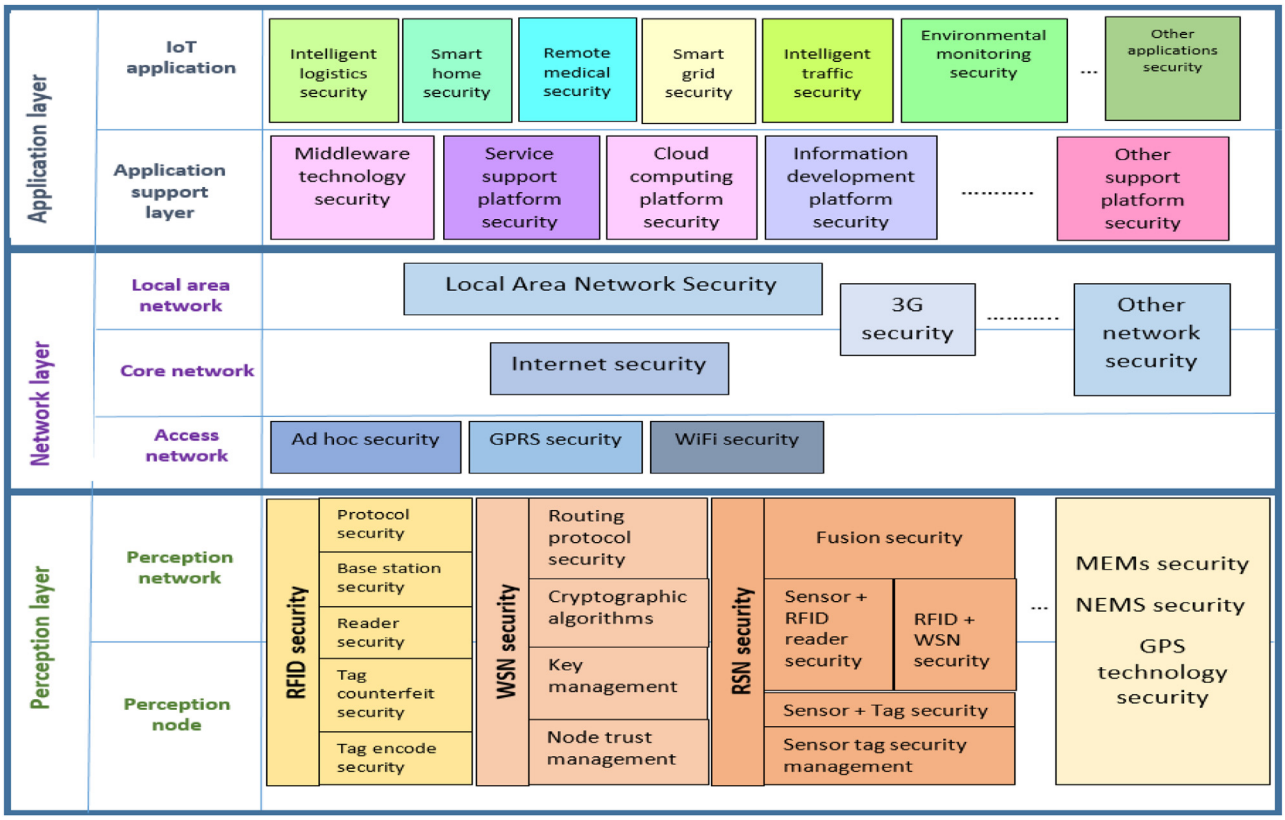

Fig. 1. Typical IoT security architecture.

In addition to the current services, the emergence of new communication technologies, such as 5G, will make the role of the Cloud become more significant. 4G and 5G cellular connectivity allows long range wireless communication. Moreover, the ability to make all IoT devices addressable by using IPV6, enables the IoT devices to be connected directly to the Cloud.

3. Introduction to IoT security

Due to the diversity of the devices and multitude of communication protocols in an IoT systems, and also various interfaces and services offered, it is not suitable to implement security mitigation based on the traditional IT network solutions. In fact, the current security measures which are applied in a conventional network may not be sufficient. Attack vectors as listed by Open Web Application Security Project (OWASP) concern the three layers of an IoT system, which are hardware, communication link and interfaces/services. Hence, the implementation of IoT security mitigation should encompass the security architecture at all IoT layers, as presented in Fig. 1. Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) are considered as part of an IoT network. Thus, possible attacks on these two systems are presented in Table 2.

3.1. IoT attack vectors

Referring to the IoT security architecture, IoT security issues are pertinent at all three IoT layers. For instance, lack of transport encryption concerns an insecure communication link between device and the Cloud, device and gateway, device and mobile applications, one device and another device, and communication between the gateway and the Cloud.

A very popular vector for gaining access to IoT devices arises due to inadequate authentication and authorization procedures. In the current IoT systems, the protocols that support authentication are MQTT, DDS, Zigbee and Zwave. Nevertheless, even if the developer has provided the authentication tools required for IoT communications, pairing and messaging, there are still opportunities for the communication to be hijacked. Furthermore, insecure network services may cause the bad actor or the threat to explore the network and propagate through it. Currently, authentication is the most popular security method to achieve secure communication in the network layer. Even though there are issues of impracticality due to the devices' constraints, some researchers suggest implementing IPSec in the IoT environment through the adaptation layer. There is also ongoing research to produce lightweight authentication based on public key management. Research in authentication will be extensively discussed in the next section.

Insufficient security configurability is due to the hardcoded credentials which are often used within IoT devices. Hardcoded credentials are easy to compromise due to the use of the same password by many devices. Poor physical security is another attack vector caused by vulnerability in the hardware. The main obstacle in encrypting the devices is due to the simplicity of devices such as sensors. Furthermore, there might be a conflict in terms of the usability of the product. However, it might be worthwhile to implement lightweight encryption in devices to ensure the confidentiality and security of the users.

Insecure web and cloud interfaces are vulnerabilities that may be an attack vector in an IoT system at the application layer. Thus, the cloud gateways have to be equipped with security controls to restrict bad actors from modifying configurations. Applying biometrics and multi-level authentication for access control might be a good solution at the application layer. Due to the changing trends in security threats, [2] has suggested current security challenges according to the layer and the possible countermeasures. Some current challenges and the proposed countermeasures are presented in Table 3. [4]

Table 2
Possible Attacks on WSN and RFID.

	RFID attacks	WSN attacks
Layer	Possible attacks	Possible attacks
Physical/Link	Jammers, replay attacks, Sybil, selective forwarding, synchronization attack.	Passive interference, active jamming of temporarily disabling the device, Sybil, destruction of RFID readers, replay attacks
Network/Transport	Sinkhole, unfairness, false routing, hello and session flooding, eavesdropping.	**Tag attacks:** Cloning, spoofing **Reader attacks:** Impersonation, eavesdropping **Network protocol attacks**
Application Layer	Injection, buffer overflows	Injection, buffer overflows, unaithorized tag reading, tag modification
Multi-layer attack	Side channel attack, replay attacks, traffic analysis, crypto attack	Side channel attack, replay attacks, traffic analysis, crypto attack

Table 3
Current challenges in IoT security and the proposed countermeasures [2].

Layer	Security challenges	Mitigation
Perception	Detection of the abnormal sensor node	fault detection algorithm, decentralized intrusion detection system
	The choice cryptography algorithms and key management mechanism to be used	public key encryption due to the large scale network slot reservation protocol Access control, mitigation of resource depletion attacks
	Data and sender anonymity	
	Device vulnerabilities	
Network	Enabling IPSec communication with IPv6 nodes	Research in the suitability of IPv6 and IPSec for secure communication.
Application	Configurable embedded computer systems.	No suggestion is available from this paper

Securing IoT systems presents a number of unique challenges, such as unreliable communications, hostile environments, and inadequate protection of data and privileges [9].

As shown in Table 3, there are more security challenges at the perception layer. This may be for several reasons, such as easy physical access to the end nodes, vulnerable devices' web interfaces, and unsecured network services. Hence, it can be concluded that for IoT systems, physical devices or the end-nodes are the main attack surface for the adversaries.

4. Development of current IoT security mechanisms

The main objective of applying security mitigation is to preserve privacy, confidentiality, ensuring the security of the users, infrastructures, data and devices of the IoT and to guarantee the availability of the services offered by an IoT ecosystem. Thus, the mitigation and countermeasures are usually applied according to the classic threat vectors. Fig. 2 shows the trends in the techniques and methods which have been used in 2016–2018. It is observed that authentication is still the most popular technique for security, while trust management is gaining popularity, due to its ability to prevent or detect malicious node. On the other hand, research on encryption is focussing on lightweight and low-cost encryption for low-power and constrained devices.

4.1. Authentication

Authentication is the process of identifying users and devices in a network and granting access to authorized persons and non-manipulated devices. Authentication is one way to mitigate attacks to the IoT systems such as the reply attack, the Man-in-the-Middle attack, the impersonation attack, and the Sybil attack. As shown in the graph in Fig. 3, authentication is currently still the most popular method (60%) to grant access to the user at the application layer and also give access to the device in the IoT network.

Transport layer Security (TLS) is widely used for communication authentication and encryption. Specifically for constrained devices, TLS offers TLS-PSK, which uses pre-shared keys, and TLS-DHE-RSA authentication method which uses RSA and Diffie-Hellman (DH) key exchange, which are public key and cryptographic protocols. In this scheme, the two entities that are to perform mutual authentication must prove their legitimacy to each other by sharing secret information (pre-shared keys) beforehand. Since only symmetric key encryption is used in the authentication process, the scheme is suitable for constrained devices such as sensors [10]. Currently, there are three types of authentication protocols designed for IoT: asymmetric-cryptosystem based protocols (Table 5), symmetric-cryptosystem based protocols (Table 6), and hybrid protocols [11].

Since the users and devices in an IoT environment create two-way communication, there is a mutual communication between the device and the servers. The device will send data to the server as well as receive control data transmitted by the server. As such, mutual authentication is crucial in an IoT system to check the validity of both the device and the server. Mutual authentications are in [12–15]. Recently, there has been a huge demand for lightweight authentication and encryption. In [13,14,16–22], the aim is to provide lightweight authentication for access control and secure communication. Multi-factor authentication by using bio-hashing and anonymity are other ways to achieve IoT authentication's goal, as suggested by [12,23,24] and [15]. Fig. 4 presents current trends in IoT authentication methods from 2016 to 2018.

4.1.1. Weaknesses of IoT authentication methods

Due to the challenges in an IoT system, such as scalability, constrained devices, heterogeneous protocols and communication channels, applying authentication as a security mechanism may face several challenges, which are discussed briefly in this section.

The Key Agreement (LKA) protocol is proposed by [22]. It is based on the Internet Key Exchange (IKEV2). This protocol is de-

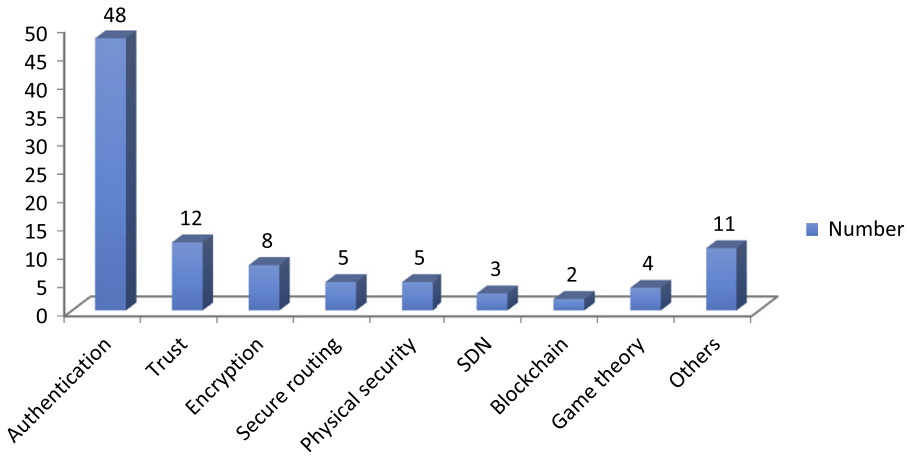

Fig. 2. Publications in IoT security from 2016 to 2018
*Publications from Elsevier, IEEE, Hindawi and Springer from 2016 until June 2018.

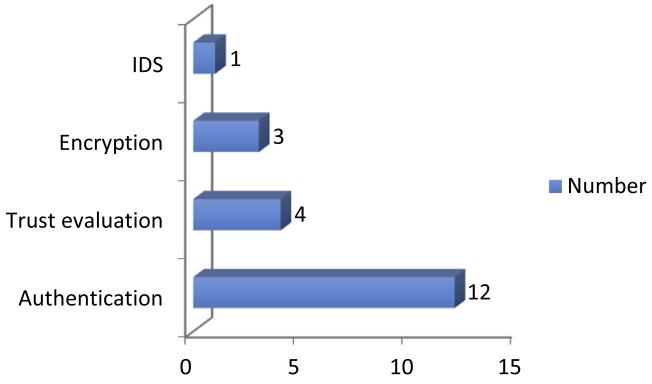

Fig. 3. Access control method according to the current IoT research.

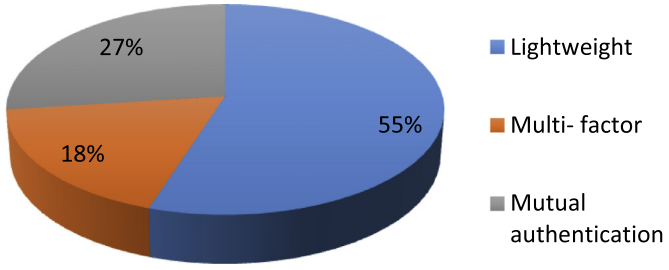

Fig. 4. Research trends on authentication.

signed to provide end-to-end security between IPv6 and 6LoWPAN nodes. However, this protocol is only applicable to IP based devices, which need to be equipped with the relevant authentication tools. On the other hand, lightweight cryptographic functions to provide lightweight and privacy-preserving mutual authentication are proposed by [14]. However, the devices need to be synchronized with the cloud server and the proposed scheme does not support dynamicity.

A secure and efficient user authentication scheme for multi-gateway wireless sensor networks is proposed by [25]. The proposed scheme supports the scalability and dynamics of a WSN without affecting the functionality of the registration or authentication process of both the user and sensor nodes and mutual authentication. Despite the advantages of the scheme, the proposed scheme has a higher computational overhead than other lightweight authentication schemes.

An enhanced authentication and key establishment scheme is designed for M2M communications in the 6LoWPAN networks (EAKES6Lo) [17]. In the proposed scheme, a hybrid cryptography approach is employed for secure authentication and flexible key establishment in the resource constrained 6LoWPAN nodes. Even though the proposed security scheme supports both static and mobile nodes in 6LoWPAN networks, the authentication scheme is energy consuming for resource-constrained devices.

An end-to-end security protocol for 6LoWPAN (6LowPSec) [16] performs security functions (cipher, integrity check, authentication etc.) only at end devices, especially for a 6LoWPAN border router, without requiring any additional network security functions. The proposed protocol is implemented at the adaptation layer and requires minimum overhead, processing, and minimum control information exchange.

A two-factor authentication and key agreement scheme in 5G-integrated WSNs for the IoT is proposed in [15] in order to support anonymity for mitigating offline password guessing attacks and other relevant attacks due to the inefficiency of the authentication process. Due to its higher computational and communication cost, the proposed authentication scheme might not applicable to normal sensor nodes.

However, all the proposed authentications are a form of one-time process and the use of a public key for lightweight authentication is still not the ultimate solution for security mitigation since a public key can be stolen [26]. Moreover, authentication may be bypassed by some malicious codes or statements. In [22] and [15] the weaknesses of the current solutions for IoT authentication are elaborated as listed below:

1) Stolen verifier attack and many logged-in users with the same login ID attack.
2) Denial-of-service attack and node capture attack.
3) Replay attack and forgery attack.
4) Stolen smart-card and sensor-node impersonation.
5) Gateway node bypassing and sensor-node key impersonation.
6) Off-line password guessing attack, off-line identity guessing attack, smart card theft attack, user impersonation attack, sensor node impersonation attack.

Even though authentication is still considered the primary security mechanism for most IoT systems, it still has weaknesses and flaws and may not be a holistic solution for IoT security mitigation. However, it is still worthwhile to look into some of the current authentication mechanisms proposed from 2016 to 2018, as presented in Table 4.

Table 4
Recent research on authentication.

Ref	Layer	Device Centric		Lightweight	U2M	M2M	Security objective	Domain	Advantage	Simulator/Computation/ Analysis tools
[15]	Network	No		Yes	Yes	Yes	Secure Communication	Generic	Overhead is reduced	Cooja
[17]	Network	Yes		No		Yes	Secure Communication	Generic	Support both mobile and static nodes, mutual authentication	MATLAB
[27]	Network	Yes		No	No	Yes	Secure Communication	Generic	Mutual authentication, three factor authentication	NS3
[28]	Network	Yes		No	Yes	Yes	Secure Communication	Generic	Improve key management and use AES-GCM one pass authentication for data integrity	Not available
[23]	Application	Yes		Yes	Yes	No	Access Control	Generic	Multi-factor authentication, lightweight biometric authentication and key agreement	AVISPA
[13]	Network	Yes		Yes	Yes	No	Access Control	WSN	Mutual authentication, novel authentication and key agreement based on bio-hashing	AVISPA
[29]	Network	Yes		No	No	Yes	Access Control	Vehicular network	Capacity based access admission control	MATLAB
[30]	Network	Yes		No	No	Yes	Secure Communication	WSN	Authentication scheme for multi gateway WSN	NS2
[31]	Network	Yes		No	Yes	No	Access Control	Generic	Three factor UAKMP	AVISPA
[18]	Network	Yes		Yes	No	Yes	Access Control	Generic	Ultra weight RFID authentication protocol	C++
[32]	Network	Yes	No		Yes	Yes	Access Control	Medical	Use elliptic curve crypto system to generate symmetric secure key	Cooja
[33]	Application	Yes	No		No	Yes	Identification	Medical	Use NFC and suitable for mobile environment	NS2
[34]	Network	Yes	No		Yes	Yes	Access Control	Medical	Interpret users' biometric signal	NS2
[35]	Network	Yes	Yes		No	Yes	Secure communication	Generic	Unidirectional and bidirectional IP or non-IP devices	MATLAB
[24]	Application	Yes	No		Yes	No	Access Control	Generic	Three factor authentication using bio-hashing	AVISPA
[36]	Network	Yes	No		No	Yes	Secure Communication	Generic	Security enhanced group based (SEGB)	AVISPA
[36]	Application	No	No		Yes	No	Access Control	Generic	Parallel matching mechanism and cloud computing based resolution	Prototype available
[37]	Network	Yes	No		No	Yes	Secure Communication	Generic	Secure network coding signatures	Not available
[20]	Application	Yes	Yes		Yes	No	Access Control	Smart Home	Lightweight authorization for un-trusted Cloud Platform	Test-bed
[13]	Network	No	No		Yes	No	Access Control	WSN	Bio hashing authentication	AVISPA
[38]	Network	Yes	No		Yes	No	Access Control	Generic	New signature based authentication key establishment	AVISPA
[39]	Application	No	No		Yes	No	Access Control	BAN	Authentication protocol by using smart card	BAN-logic and AVISPA
[40]	Network	Yes	Yes		No	Yes	Secure communication	BAN	Mutual authentication	Not Available
[21]	Physical	Yes	Yes		No	Yes	Attestation and identification	Generic	Software integrity, mutual authentication and tamper proof feature for smart embedded object	Prototype
[41]	Physical	Yes	Yes		No	Yes	Secure communication	Generic	Social networking based authentication (SNAuth) protocol	OPNET
[42]	Network	Yes	No		No	Yes	Secure communication	Generic	Identity based AKE protocol	Not available
[43]	Network	Yes	No		No	Yes	Secure communication	Generic	No pre configured security information is needed	MICA2
[44]	Application	No	No		Yes	No	Access Control	Medical	Provide user anonymity	Test-bed
[10]	Network	Yes	No		No	Yes	Secure Communication	Generic	ID-based key sharing scheme to TLS	Not available
[22]	Application	No	Yes		Yes	No	Access control	Generic	Certificate free authentication	MATLAB
[45]	Network	Yes	No		No	Yes	Secure Communication	VANET	certificate-less authentication	Not available

Table 5
Asymmetric lightweight cryptography algorithms for IoT [47].

Asymmetric algorithm	Key size	Code length	Possible attack
RSA	1024	900	Modules attack
ECC	160	8838	Timing attack

4.2. Encryption

In achieving end to end security, the nodes are encrypted. However, due to the heterogeneity of the IoT systems, some nodes might be able to embed general purpose micro processors. However, low resources and constrained devices can only embed application-specific ICs [46]. Hence, conventional cryptographic primitives are not suitable for low-resource smart devices due to their low computation power, limited battery life, small size, small memory, and limited power supply. Thus, lightweight cryptography may be an efficient encryption for these devices.

Since the goal for IoT encryption is to achieve efficient end to end communication with low power consumption, symmetric and asymmetric lightweight algorithms for IoT are designed to meet the requirements [47]. Research in [48–50] has focussed on implementing low cost and lightweight encryption in the physical and the network. On the other hand, an attribute based decryption system is proposed by [49] to support user revocation. A summary of recent research on encryption is presented in Table 7.

4.3. Trust management

There has been an increasing amount of publications on devices' trust management. The objective of IoT trust management is to detect and eliminate malicious nodes and to provide secure access control. Automated and dynamic trust calculations to validate the trust values of the participating nodes in an IoT network are among the state of the art in trust management research. However, most of the research focuses on detecting the malicious nodes; only a few trust based access control method have been proposed. Indeed, due to scalability and the huge number of smart things which hold sensitive data, there is an urgent need for an automated, transparent and easy access control management, so that different access level can be given to different nodes/users [56].

Even though only 20% (refer to Fig. 3) of the access control methods currently use trust evaluation, it is still a promising security mechanism. This may be due to its ability to calculate a node's dynamic trust score [57]. This enables the trust value of each node to be progressively evaluated. Moreover, Caminha et al. in [58] have proposed smart trust evaluation by using Machine Learning (ML). This may be able to mitigate the on-off attack which threatens the node's trust value. In addition, trust management might be able to complement the obvious weakness of authentication, such as attacks from the corrupted nodes.

Zhang et al. [59] state that trust computing for access control in an IoT network, Trust-Based Access Control (TBAC), is still relatively new but has been implemented successfully in commercial applications. Bernal et al. [60] proposed a trust-aware control system for IoT that promotes multidimensional trust properties. Due to the devices' resource constraints, the trust evaluation is centralized as in many proposals, see Table 8.

4.4. Secure routing

Sensors and actuators are important elements in an IoT network. Even though these devices are usually low-powered and resource constrained, they are self-organized and share information. At the same time, they also act as data storage and perform some computations. Hence, scalability, being able to be autonomous, and energy efficiency are important for any routing solution. Some of these sensor nodes are border routers to connect the low power lossy network (LLN) to the internet or to a close by Local Area Network (LAN). Due to the large scale of the IoT networks, the IP addresses for these devices are based on IPv6. IPv6 over low power wireless personal area networks (6LoWPAN) is an IETF IPv6 adaptation layer that enables IP connectivity over low power and lossy network. However, since there is no authentication at the 6LoWPAN layer, there is a high likelihood of a security breach [69].

RPL (Low power and lossy network protocol) is designed for multipoint communication while supporting both point to point and multi point communication in an LLN. DODAG (Destination Oriented Directed Acyclic Graph) is the RPL topology for the nodes' routing protocol. Even though RPL meets all the routing requirements of LLNs, it is susceptible to many security attacks, as summarized in Table 9.

In order to launch a Sinkhole, Blackhole or Sybil attack, a malicious node will try to find a way to participate in the routing or forwarding path of the data and control packets. Thus, it will exploit the vulnerabilities of the routing protocols which are designed with the assumption that all the participating nodes are trustworthy [71].

A secure and efficient protocol for route optimization is proposed in [72]. The proposed protocol is to optimize the existing routing protocol in Proxy Mobile IPv6 (PMIPv6) in a Smart Home network. The protocol supports mutual authentication, key exchange, perfect forward secrecy, and privacy. A novel secure-trust aware RPL routing protocol (SecTrust-RPL) which is based on the trust mechanism is proposed and implemented in [73]. The proposed protocol is to provide protection against Rank and Sybil attacks while optimizing network performance.

A secure time synchronization model for large-scale IoT is proposed in [27], in which a node uses its father node and grandfather node to detect any malicious node. A secure and trust-based approach to mitigate the Blackhole attack on AODV based MANET is proposed in [74].

Even though the efficiency of the proposed protocols is evaluated and performance metrics such as throughputs are increased, the end to end delay may increase due to isolation and the computational process and may not support scalability and mobility, which are critical aspects of an IoT system.

Due to the vulnerabilities of a RPL routing protocol, current related work for secure routing is presented in Table 10.

Table 6
Symmetric lightweight cryptography algorithms for IoT [47].

Symmetric algorithm	Code length	Structure	Number of rounds	Key size	Block size	Possible attacks
AES	2606	SPN	10	128	128	Man-in-the-middle attacks
HEIGHT	5672	GFS	32	128	64	Saturation attack
TEA	1140	Feistel	32	128	64	Related key attack
PRESENT	936	SPN	32	80	64	Differential attack
RC5	Not fixed	ARX	20	16	32	Differential attack

Table 7
Current research on encryption based solution.

Ref	Layer	Security objective	Domain	Advantage	Simulator/Computation/ Analysis tools
[48]	Physical	Secure 802.15.4 transceiver design	Generic	Reduces computations at the upper layer and mitigate multiple attacks	ASIC UMC 018 u CMOS and FPGA prototype
[49]	Network	To maintain data confidentiality	Generic	Low cost	Not available
[51]	Application	Access control	Generic	Attribute based decryption with user revocation	MICA
[52]	Network	To prevent energy depletion	Generic	Accurate localization of the attacker	Test-bed
[53]	Physical	Data protection	Generic	High-speed ultra low-power low energy with multiple levels of security	Test-bed
[50]	Network	Data protection	Generic	Lightweight	NS2
[54]	Physical	Secure communication	Industrial	Detect multiple counterfeit ICs	Prototype
[55]	Physical	Access control	WBAN	Heterogeneous sign-cryption scheme	Not available

Table 8
Current research on trust based solution.

Ref	Layer	Centralized	Decentralized	Advantage	Simulator/Computation/Analysis tools
[61]	Network	Yes		Trust computation defines the direct trust of a node on its neighbour.	Not available
[57]	Network		Yes	Dynamic trust calculation	NS3
[62]	Network	Yes		More reliable trust calculation	NS3, MATLAB
[63]	Network			Semi distributed	MATLAB
[64]	Network	Yes		Time based trust aware routing protocol	Cooja
[65]	Network	Yes		Lightweight trust evaluation for the nodes to detect malicious node	MATLAB
[66]	Network	Yes		Trust evaluation is based on nodes' behaviour and historical trust.	OMNET++
[67]	Network		Yes	Trust management from devices' property by using Fuzzy approach	MATLAB Fuzzy Toolbox
[58]	Network	Yes		Smart trust management by using Machine Learning and elastic slide window	Cooja
[68]	Network		Yes	Multi domain RFID system	NS3

Table 9
Attacks on RPL [70].

Attack	Effect on network parameter
Selective forwarding	Disrupt routing path
Sinkhole	Large traffic flows through attacker node
Hello flooding	Route formation through attacker node
Warmhole	Disrupt the network topology and traffic flow
Sybil and clone ID	Routing traffic unreachable to victim node
Denial of service	Make resources unavailable to intended users
Blackhole	Packet delay and control overhead
Rank	Packet delay, delivery ratio and generation of un-optimized path and loop
Version number	Control overhead, delivery ratio, end to end delay
Local repair	Control overhead, disrupt routing and traffic flow
Neighbour and DIS	Packet delay

Table 10
Recent research on secure routing.

Ref	Objective	Method	Simulator/Computation/Analysis tools
[75]	Secure routing	Mutual authentication, key exchange, perfect forward secrecy and privacy.	AVISPA
[27]	Anomaly detection	Secure time synchronization model	NS2
[76]	To prevent gray-hole attack	Enhanced DCFM method	NS3
[64]	To mitigate rank and Sybil attack	Time-based trust aware RPL (SecTrust RPL)	Cooja
[77]	Data confidentiality	Hybrid control channel based cognitive AODVrouting protocol with directional antenna	NS2

4.5. New technology

There are two types of new technology which have been of interest recently. SDN (software defined network) and blockchain are among the popular new technologies that converge with IoT security solutions. The main idea of SDN is to separate the network control and the data control. Thus, both centralized control and dynamic management of the network are possible, in order to deal with obstacles in the IoT environment such as resource allocation in IoT devices. Furthermore some current challenges in IoT, such as reliability, security, scalability and QoS might be able to be addressed efficiently.

Block chain is the backbone of cryptocurrency. IoT based applications will take the advantage of its secure and private transactions, as well as its decentralization of communications and processes. To date, its application has achieved significant success in financial applications. Decentralization, pseudononymity and secure transactions are among the advantages of blockchain technology for the IoT.

Kim et al. [78] proposed an SDN based cloud to provide safe data transmission with QoS. In order to deal with non-patchable vulnerabilities, *Ge* et al. [79] proposed to change the attack surface of the IoT network in order to increase the attack effort by using SDN. In [80] block chain technology is used to create secure virtual zones where things can identify and trust each other. Self-organization Blockchain Structures (BCS) are designed to establish the relationship between blockchain and IoT, as proposed in [81]. Ra et al., in [82], use block chain technology to provide confidentiality in a smart home environment. Table 11 presents other methods or technologies used currently for IoT security, which includes physical layer security.

5. Discussion

This survey intended to give an overview of the current trends in IoT security research. At the same time, this survey presented some attack vectors and challenges to IoT security. High quality papers from Web of Knowledge were reviewed and categorized into by their objectives, methods used in the research, and the simulation tools used in order to simulate or validate the results. It was found that other than the simulation tools and modeller, the availability of the platform to validate the security protocol will help in producing a novel IoT security protocol. Hence, there is no doubt that the rapid progress of research in IoT security is supported by the availability of simulation tools and IoT modellers.

There have been real catastrophic events resulting from attackers using insecure devices as “thingbots” to attack the IoT network. This is strong evidence that the security of the IoT is of pressing concern. It is also assumed that the IoT will remain a target and attack vector for years to come. This is due to the increasing number of IoT devices, the heterogeneity of the protocols used in the IoT, and the minimal or default security measures embedded in the devices by the manufacturers. Clearly, cyber (IT) security, such as authentication, encryption, and firewalls, should be implemented as security measures in the IoT. But this is not sufficient. The interaction and integration between physical and cyber systems make the IoT different from the traditional network.

New vulnerabilities, such as unsecured communication channels, the presence of malicious activities in the network, and unsecured physical devices, introduce new type of threats to the IoT networks. This also evidences that IoT devices are the targets of surface attacks due to their irregular patching and updates: often the devices come with minimal or maybe no authentication or encryption at all. Furthermore, usually these devices are deployed in a hostile environment and available at all times; hence there may be minimal or no protection against any illegal physical access.

Table 11
Other methods which are used in the recent research.

Ref	Layer	Objective	Method	Domain	Simulator/Computation/Analysis tools
[83]	Network	Maximum security pay offs	Game theory	Generic	Not available
[84]	Network	Lightweight anomaly detection	Game theory	Generic	Not available
[85]	Network	To detect DoS	Game theory	WSN	NS2
[86]	Network	Secure communication	TCP/IP based comm.	Generic	Testbed
[87]	Network	Privacy	Location privacy algorithm	Generic	Not available
[88]	Network	Anomaly detection	Network scanning	Generic	NS3, MATLAB
[89]	Network	GPS spoofing	Hybrid localization	Drones	Open CV
[90]	Network	Anomaly detection	HIST and Game theory	Generic	TOSSIM and AVRORA
[91]	Network	Data integrity	Linear network coding	Generic	MATLAB
[92]	Physical	Location spoofing	Geo-spatial tagging algorithm	Generic	Testbed
[35]	Physical	Security tagging	System hardening	Generic	Prototype
[93]	Multi layer	Security analysis	Mathematical modelling	Generic	No
[94]	Network	Secure communication	Enhancing MQTT	Generic	Testbed
[95]	Network	Malicious node detection	Mathematical algorithm	Industrial	OMNet, MATLAB
[96]	Physical	Mitigate eavesdropper	Physical layer security	Generic	C++
[97]	Physical	Securing uplink transmission	UOSPR lightweight single antenna	Generic	NS3, MATLAB
[98]	Physical	Secure transmission	Cooperative jamming	Generic	MATLAB
[99]	Network	IDS	Heterogeneous access control protocol	Generic	Not available

Authentication and encryption may be effective solutions in mitigating security issues in IoT. However, for low-power, computationally and resource constrained devices, the implementation of effective authentication and encryption is still in its infancy and does not guarantee the prevention of malicious nodes in the network, such as corrupted devices or machines. Furthermore, due to its convenience, manufacturers usually apply hardcoded credentials or passwords, something which typically leads to a significant authentication failure. From this survey, it is seen that current research on devices' security has mainly focused on improving lightweight authentication and encryption for low-power and resource constrained devices.

On the other hand, securing the routing protocol at the network layer and implementing trust and reputation based malicious node detection suffers end-to-end delay, communication overhead, and a high false positive rate.

The findings from this survey demonstrate that even though authentication alone may not be sufficient for IoT security, the current trend of IoT security mechanisms is to work on lightweight, mutual and multi-factor authentication, especially at the network and application layers. On the other hand, in order to mitigate devices' security issues, lightweight and low cost encryption are proposed for the physical layer.

In conclusion, according to the IoT security architecture, security mitigation encompasses all the layers in the basic IoT architecture, namely, perception, network, and application, even though it is observed that most of the current mechanisms are applied to the network layer. It also can be concluded that an appropriate IoT threat modelling might be useful in strategizing effective IoT security mitigation.

6. Conclusion

The purpose of this survey has been accomplished by giving an adequate overview of the research trends in IoT security between 2016 until 2018 and the relevant tools and simulators. The research from reputable publishers have been reviewed and categorized for easy reference for new researchers. Future directions of this research include developing a comprehensive IoT threat modelling, followed by designing a zero trust algorithm to mitigate known and unknown cyber-attacks on an IoT system.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.comnet.2018.11.025.

References

[1] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, W. Shi, On security challenges and open issues in Internet of Things, Futur. Gener. Comput. Syst. 83 (2018) 326–337.
[2] H.Z. Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, A survey on security and privacy issues in internet-of-things, in: 2015 10th Int. Conf. Internet Technol. Secur. Trans., 4, 2015, pp. 202–207.
[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142.
[4] A. Tewari, B.B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, Futur. Gener. Comput. Syst. (2018) 1–13, doi:10.1016/j.future.2018.04.027.
[5] A. Riahi Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the Internet of Things, Digit. Commun. Networks 4 (2) (2018) 118–137.
[6] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: A survey, J. Netw. Comput. Appl. 88 (2017) 10–28 December 2016.
[7] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: A top–down survey, Comput. Networks 141 (2018) 199–221.
[8] M. Chernyshev, Z. Baig, O. Bello, S. Zeadally, Internet of Things (IoT): Research, IEEE Internet of Things Journal 5 (3) (2018) 1637–1647.
[9] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, Y. Jin, Internet-of-Things Security and Vulnerabilities : Taxonomy, Challenges, and Practice, Journal of Hardware and Systems Security 2 (2018) 97–110.
[10] T. Shinzaki, I. Morikawa, Y. Yamaoka, Y. Sakemi, IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data, Fujitsu Sci. Tech. J. 52 (4) (2016) 52–60.
[11] M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, Authentication Protocols for Internet of Things: A Comprehensive Survey, Security and Communication Networks 2017 (2017) 1–41.
[12] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K.R. Choo, A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things, IEEE Internet of Things Journal 5 (3) (2018) 1606–1615.
[13] J. Srinivas, S. Mukhopadhyay, D. Mishra, Ad Hoc Networks Secure and efficient user authentication scheme for multi-gateway wireless sensor networks, Ad Hoc Networks 54 (2017) 147–169.
[14] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, J. Shen, A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server, Comput. Electr. Eng. 63 (2017) 168–181.
[15] S. Shin, T. Kwon, Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks, IEEE Access 6 (2018) 11229–11241.
[16] G. Glissa, A. Meddeb, 6LowPSec: An End-to-End Security Protocol for 6LoWPAN, Ad Hoc Networks 82 (2018) 100–112.
[17] Y. Qiu, M. Ma, A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks, IEEE Trans. Ind. Informatics 12 (6) (2016) 2074–2085.
[18] M. Safkhani, N. Bagheri, Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things, J. Supercomput. 73 (8) (2017) 3579–3585.
[19] R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, S. Member, Security Access Protocols in IoT Capillary Networks, IEEE Internet of Things Journal 4 (3) (2017) 645–657.
[20] B. Chifor, I. Bica, V. Patriciu, F. Pop, A security authorization scheme for smart home Internet of Things devices, Futur. Gener. Comput. Syst. 86 (2018) 740–749.

[21] W. Feng, Y. Qin, S. Zhao, D. Feng, AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS, Comput. Networks 134 (2018) 167–182.

[22] M. Lavanya, V. Natarajan, Lightweight key agreement protocol for IoT based on IKEv2, Comput. Electr. Eng. 64 (2017) 1339–1351.

[23] P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications 34 (2017) 255–270.

[24] R. Amin, S.K. Hafizul, G.P. Biswas, M. Khurram, L. Leng, N. Kumar, Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Comput. Networks 101 (2016) 42–62.

[25] J. Srinivas, S. Mukhopadhyay, D. Mishra, Secure and efficient user authentication scheme for multi-gateway wireless sensor networks, Ad Hoc Networks 54 (2017) 147–169.

[26] V.S. Latha Tamilselvan, Prevention of blackhole attack in MANET, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), 2007.

[27] T. Qiu, et al., A Secure Time Synchronization Protocol Against Fake Timestamps for Large-Scale Internet of Things, IEEE Internet of Things Journal 4 (6) (2017) 1879–1889.

[28] A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, D. Toal, A secure end–to-end IoT solution, Sensors Actuators A. Phys. 263 (2017) 291–299.

[29] J.P.D. Comput, M. Tao, K. Ota, M. Dong, Z. Qian, AccessAuth : Capacity-aware security access authentication in federated-IoT-enabled V2G networks, J. Parallel Distrib. Comput. 118 (2018) 107–117.

[30] F. Wu, et al., An e ffi cient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment, J. Netw. Comput. Appl. 89 (2017) 72–85 November 2016.

[31] M. Wazid, A.K. Das, V. Odelu, N. Kumar, M. Conti, M. Jo, Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks, IEEE Internet Things J 5 (1) (2018) 269–282.

[32] Z. Mahmood, H. Ning, Applied sciences secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT, Applied Sciences (7) (2017) 1–22.

[33] M. Wazid, A. Das, M. Khan, Secure authentication scheme for medicine anti–counterfeiting system in IoT environment, IEEE Internet of Things Journal 4 (5) (2017) 1634–1646.

[34] L. Yeh, W. Tsaur, H. Huang, Secure IoT-Based, Incentive-aware emergency personnel dispatching scheme with weighted fine-grained, ACM Transactions on Intelligent Systems and Technology 9 (1) (2017) 1–23.

[35] S. Choi, C. Yang, J. Kwak, System hardening and security monitoring for iot devices to mitigate iot security vulnerabilities and threats, KSII Transactions on Internet and Information Systems 12 (2) (2018) 906–918.

[36] B.L. Parne, S. Member, S. Gupta, S. Member, SEGB : Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE / LTE-A Network, IEEE Access 6 (2018).

[37] T. Li, W. Chen, Y. Tang, H. Yan, A homomorphic network coding signature scheme for multiple sources and its application in IoT, Security and Communication Networks 2018 (2018).

[38] S. Challa, M. Wazid, A.K. Das, Secure signature-based authenticated key establishment scheme for future IoT Applications, IEEE Access 5 (2017).

[39] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, V. Chang, A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment, Futur. Gener. Comput. Syst. 78 (2018) 1005–1019.

[40] M. Nikravan, A. Movaghar, M. Hosseinzadeh, A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks, Wirel. Pers. Commun. 99 (2) (2018) 1035–1059.

[41] N.N. Dao, Y. Kim, S. Jeong, M. Park, S. Cho, Achievable multi-security levels for lightweight iot-enabled devices in infrastructureless peer-aware communications, IEEE Access 5 (2017) 26743–26753.

[42] O. Ruan, Y. Zhang, M. Zhang, J. Zhou, L. Harn, After-the-fact leakage-resilient identity-based, IEEE Systems Journal 12 (2) (2018) 2017–2026.

[43] K.W. Kim, Y.H. Han, S.G. Min, An authentication and key management mechanism for resource constrained devices in IEEE 802.11-based IoT Access Networks, Sensors (Switzerland) 17 (10) (2017) 1–14.

[44] C.T. Li, T.Y. Wu, C.L. Chen, C.C. Lee, C.M. Chen, An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system, Sensors (Switzerland) 17 (7) (2017).

[45] H. Tan, D. Choi, P. Kim, S. Pan, I. Chung, Secure certificateless Authentication and road message dissemination protocol in VANETs, Wirel. Commun. Mob. Comput. (2018) 1–14.

[46] M. Katagi, S. Moriai, Lightweight cryptography for the internet of things, 2008, pp. 7–10. Technical paper by SONY Corporation.

[47] S. Singh, Advanced lightweight encryption algorithms for IoT devices : survey, challenges and solutions, J. Ambient Intell. Humaniz. Comput. 0 (0) (2017) 0.

[48] A.K. Nain, J. Bandaru, M.A. Zubair, R. Pachamuthu, A secure Phase-Encrypted IEEE 802. 15. 4 Transceiver Design, IEEE Transactions on Computers 66 (8) (2017) 1421–1427.

[49] M. Mangia, F. Pareschi, R. Rovatti, Low-cost security of IoT sensor nodes with rakeness-based compressed sensing : statistical and known-plaintext attacks, IEEE Transactions on Infromation Forensics and Security 13 (2) (2018) 327–340.

[50] Z. Mahmood, H. Ning, A.U. Ghafoor, A polynomial subset-based efficient multi-party key management system for lightweight device networks, Sensors (Switzerland) 17 (4) (2017) 2–20.

[51] Z. Qin, J. Sun, D. Chen, H. Xiong, Flexible and lightweight access control for online healthcare social networks in the context of the internet of things, Mobile Information Systems 2017 (2017).

[52] X. Cao, D.M. Shila, S. Member, Y. Cheng, S. Member, Ghost-in-ZigBee : Energy depletion attack on ZigBee-based wireless networks, IEEE Internet of Things Journal 3 (5) (2016) 816–829.

[53] D.H. Bui, D. Puschini, S. Bacles-Min, E. Beigne, X.T. Tran, AES datapath optimization strategies for low-power low-energy multisecurity-level internet-of-things applications, IEEE Trans. Very Large Scale Integr. Syst. 25 (12) (2017) 3281–3290.

[54] K.U.N. Yang, D. Forte, M.M. Tehranipoor, CDTA : A Comprehensive solution for counterfeit detection, traceability, and authentication in the IoT Supply Chain, ACM Transactions on Design Automation of Electronics Systems 22 (3) (2017).

[55] A.A. Omala, A.S. Mbandu, K.D. Mutiria, C. Jin, F. Li, Provably secure heterogeneous access control scheme for wireless body area network, J. Med. Syst. 42 (6) (2018) 108.

[56] I. Ishaq, IETF standardization in the field of the Internet of Things (IoT): A survey, J. Sens. Actuator Netw 2 (2013) 235–287.

[57] B. Gong, Y. Zhang, Y. Wang, A remote attestation mechanism for the sensing layer nodes of the Internet of Things, Futur. Gener. Comput. Syst. 78 (2018) 867–886.

[58] J. Caminha, A. Perkusich, M. Perkusich, A smart trust management method to detect on-off attacks in the internet of things, Secur. Commun. Networks 2018 (3) (2018) 1–10.

[59] Y. Zhang, X. Wu, Access Control in Internet of Things: A Survey, Cryptography and Security (1) (2016) 1–15.

[60] J. Bernal Bernabe, J.L. Hernandez Ramos, A.F. Skarmeta Gomez, TACIoT: multidimensional trust-aware access control system for the Internet of Things, Soft Comput 20 (5) (2016) 1763–1779.

[61] Z.A. Khan, J. Ullrich, P. Herrmann, A trust-based resilient routing mechanism for the Internet of Things, in: Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES, 2017, pp. 1–6.

[62] J.I. Chen, Embedding the MRC and SC Schemes into Trust Management Algorithm Applied to IoT Security Protection, Wirel. Pers. Commun. 99 (1) (2018) 461–477.

[63] V. Suryani, S. Sulistyo, W. Widyawan, Internet of things (IoT) framework for granting trust among objects, J. Inf. Process. Syst. 13 (6) (2017) 1613–1627.

[64] D. Airehrour, J.A. Gutierrez, S. Kumar, SecTrust -RPL : A secure trust-aware RPL routing protocol for Internet of Things, Future Generation Computer Systems (2018) (2018) 1–17.

[65] N.E. Rikli, A. Alnasser, Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks, Int. J. Distrib. Sens. Networks 12 (7) (2016) 1–16.

[66] Z. Chen, L. Tian, C. Lin, Trust model of wireless sensor networks and its application in data fusion, Sensors (17) (2017) 703–719.

[67] N.A. Mhetre, A.V. Deshpande, P.N. Mahalle, Trust management model based on fuzzy approach for ubiquitous computing, Int. J. Ambient Comput. Intell. 7 (2) (2016) 33–46.

[68] X. Wu, F. Li, A multi-domain trust management model for supporting RFID applications of IoT, PLoS One 12 (7) (2017) 1–23.

[69] D. Airehrour, J. Gutierrez, S.K. Ray, Secure routing for internet of things: A survey, J. Netw. Comput. Appl. 66 (2016) 198–213.

[70] P. Pongle, G. Chavan, A survey: Attacks on RPL and 6LoWPAN in IoT, 2015 Int. Conf. Pervasive Comput. Adv. Commun. Technol. Appl. Soc. ICPC 2015 00 (2015) 978–983.

[71] S. Djahel, F. Naït-Abdesselam, Z. Zhang, Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges, IEEE Commun. Surv. Tutorials 13 (4) (2011) 658–672.

[72] D. Shin, V. Sharma, J. Kim, S. Kwon, I. You, Secure and efficient protocol for route optimization in PMIPv6-Based SMART HOME IoT networks, IEEE Access 5 (2017) 11100–11117.

[73] D. Airehrour, J.A. Gutierrez, S.K. Ray, SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things, Futur. Gener. Comput. Syst. (2018) 1–17.

[74] M.B.M. Kamel, I. Alameri, A.N. Onaizah, STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET, in: *Proc. 2017 IEEE 2nd Adv. Inf. Technol. Electron. Autom. Control Conf. IAEAC 2017*, no. April, 2017, pp. 1278–1282.

[75] D. Shin, V. Sharma, J. Kim, S. Kwon, I. You, S. Member, Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks, IEEE Access 5 (2017) 11110–11116.

[76] N. Schweitzer, A. Stulman, R.D. Margalit, A. Shabtai, Contradiction based gray–hole attack minimization for Ad-Hoc Networks, IEEE Transactions on Mobile Computing 16 (8) (2017) 2174–2183.

[77] S. Anamalamudi, A. Rashid, M. Alkatheiri, A. Mohammed, AODV routing protocol for Cognitive radio access based Internet of Things (IoT), Futur. Gener. Comput. Syst. 83 (2018) 228–238.

[78] S. Kim, W. Na, Safe Data Transmission Architecture Based on Cloud for Internet of Things, Wirel. Pers. Commun. 86 (1) (2016) 287–300.

[79] M. Ge, J.B. Hong, S.E. Yusuf, D.S. Kim, Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities, Futur. Gener. Comput. Syst. 78 (2018) 568–582.

[80] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, M. Tahar Hammi, Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142.

[81] C. Qu, M. Tao, J. Zhang, X. Hong, R. Yuan, Blockchain based credibility verification method for IoT entities, IEEE Transaction on Information Forensics and Security 2018 (2018) 1–11.
[82] G.J. Ra, I.Y. Lee, A study on KSI-based authentication management and communication for secure smart home environments, KSII Trans. Internet Inf. Syst. 12 (2) (2018) 892–905.
[83] H. Wu, W. Wang, Detection method for internet of things systems, IEEE Transactions on Information and Security 13 (6) (2018) 1432–1445.
[84] H. Sedjelmaci, S.M. Senouci, An accurate security game for low-resource IoT devices, IEEE Transactions on Vehicular Technology 66 (10) (2017) 9381–9393.
[85] F. Yazdankhah, An intelligent security approach using game theory to detect DoS attacks in IoT, International Journal of Advanced Computer Science and Applications (8) (2017) 313–318 September.
[86] J. Jeong, D.H. Park, J.Y. Lee, U.G. Offong, S. Oh, Y. Son, Design and implementation of the intelligent convergence security system for hazard event on IoT environments 11 (4) (2018) 169–178.
[87] G. Sun, et al., Efficient location privacy algorithm for Internet of Things (IoT) services and applications, J. Netw. Comput. Appl. 89 (2017) 3–13 September 2016.
[88] L. Metongnon, R. Sadre, Fast and efficient probing of heterogeneous IoT networks, Int. J. Network Management (July 2017) (2018) 1–19.
[89] D. He, Y. Qiao, S. Chan, N. Guizani, Flight security and safety of drones in airborne fog computing systems, IEEE Communication (May 2018) (2018) 66–71.
[90] L. Yang, C. Ding, M. Wu, K. Wang, Robust detection of false data injection attacks for data aggregation in an Internet of Things-based environmental surveillance, Computer Networks 129 (2017) 410–428.
[91] L. Shi, Y. Wang, Secure data delivery with linear network coding for multiple multicasts with multiple streams in internet of things, Security and Communication Networks 2018 (2018) 1–13.
[92] P. Zhang, S.G. Nagarajan, I. Nevat, Secure Location of Things (SLOT): mitigating localization spoofing attacks in the internet of things, IEEE Internet of Things Journal 4 (6) (2017) 2199–2206.
[93] M. Ge, J.B. Hong, W. Guttmann, D.S. Kim, A framework for automating security analysis of the internet of things, J. Netw. Comput. Appl. 83 (2017) 12–27 April 2016.
[94] H. Cheon, H. Jisu, P. Jin, G. Shon, Design and Implementation of a Reliable Message Transmission System Based on MQTT Protocol in IoT, Wirel. Pers. Commun. 91 (4) (2016) 1765–1777.
[95] J. Yang, F. Zhang, W. Hu, C. Engineering, Multi-level detection and warning module for bandwidth consumption attacks, International Journal of Security and Its Application 10 (8) (2016) 181–190.
[96] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," vol. 13, no. 3, pp. 1281–1293, 2016.
[97] B. Chen, et al., Securing uplink transmission for lightweight single-antenna ues in the presence of a massive MIMO eavesdropper, IEEE Access 4 (2016) 5374–5384.
[98] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in ciot networks," pp. 1–19, 2016.
[99] M.M. Rathore, A. Paul, A. Ahmad, N. Chilamkurti, W.H. Hong, H.C. Seo, Real–time secure communication for Smart City in high-speed Big Data environment, Futur. Gener. Comput. Syst. 83 (2018) 638–652.

Mardiana binti Mohamad Noor is currently pursuing her PhD specializing in IoT security in Universiti Teknologi Malaysia. Her research interests include mathematical threat modelling, zero trust networks and cyber security. Her first degree was from Universiti Sains Malaysia in Electronics Engineering (Hons.). She completed her Masters Degree in Wireless Networks Security and attained MPhil from University Teknologi Malaysia, Kuala Lumpur (UTM KL). Mphil from Universiti Teknologi Malaysia

Wan Haslina Hassan presently overseeing the Communication Systems and Networks Research Group, in UTM KL, comprising senior academics, researchers and postgraduates students. Research facilities include network simulators and emulator - Tetcos NetSim & NS2 and Matlab. Currently developing a Cybersecurity Research Lab in collaboration with RSA Security - a global Fortune 500 company. Areas of expertise include computer/mobile/bio-communications and information/network security; curriculum design and development, research management and other activities related to research, academic administration and higher education (undergraduate and postgraduate levels) development. Experienced in supervising postgraduates students in the areas of nano/molecular communications, content-centric networks, intelligent architectures for mobility management, and network security.