Hindawi
Security and Communication Networks
Volume 2017, Article ID 6562953, 41 pages
https://doi.org/10.1155/2017/6562953

Review Article

Authentication Protocols for Internet of Things: A Comprehensive Survey

Mohamed Amine Ferrag,[1,2] Leandros A. Maglaras,[3] Helge Janicke,[3] Jianmin Jiang,[4] and Lei Shu[5,6]

[1] *Department of Computer Science, Guelma University, BP 401, 24000 Guelma, Algeria*
[2] *Networks and Systems Laboratory, Badji Mokhtar University, BP 12, 23000 Annaba, Algeria*
[3] *School of Computer Science and Informatics, Cyber Security Centre, De Montfort University, Leicester, UK*
[4] *Research Institute for Future Media Computing, Shenzhen University, Shenzhen, China*
[5] *Guangdong University of Petrochemical Technology, Guangdong, China*
[6] *School of Engineering, University of Lincoln, Lincoln, UK*

Correspondence should be addressed to Leandros A. Maglaras; leandrosmag@gmail.com

Received 27 April 2017; Accepted 28 September 2017; Published 6 November 2017

Academic Editor: Mahmoud Ghorbel

In this paper, a comprehensive survey of authentication protocols for Internet of Things (IoT) is presented. Specifically more than forty authentication protocols developed for or applied in the context of the IoT are selected and examined in detail. These protocols are categorized based on the target environment: (1) Machine to Machine Communications (M2M), (2) Internet of Vehicles (IoV), (3) Internet of Energy (IoE), and (4) Internet of Sensors (IoS). Threat models, countermeasures, and formal security verification techniques used in authentication protocols for the IoT are presented. In addition a taxonomy and comparison of authentication protocols that are developed for the IoT in terms of network model, specific security goals, main processes, computation complexity, and communication overhead are provided. Based on the current survey, open issues are identified and future research directions are proposed.

1. Introduction

The forecasters believe that the Internet of Things (IoT) holds great promise for many life-improving applications. According to forecasts from Cisco Systems [1], by 2020, the Internet will consist of over 50 billion connected things, including sensors, actuators, GPS devices, mobile devices, and all smart things that can be envisioned in the future. Currently, IBM has decided to combine several products and services into a product called IoT Solutions Practice [2] to allow the customers to find all IBM IoT offers at the same location. For example, IBM offers the Watson IoT platform [3], which combines scanning, security, and blockchain technology for authentication with a set of APIs such as IBM's SoftLayer cloud infrastructure [4]. The IoT can be realized under three scopes, namely, Internet-oriented (middleware), things-oriented (sensors), and semantic-oriented (knowledge) [5]. According to Atzori et al. [6], IoT can be represented as a three-layered architectural model, which consists of the application layer, the network layer, and the sensing layer.

As shown in Figure 1, IoT has made its entrance in four fields, including (1) Machine to Machine Communications (M2M), (2) Internet of Vehicles (IoV), (3) Internet of Energy (IoE), and (4) Internet of Sensors (IoS). M2M is a technology crucial for the realization of IoT, which is based on different protocols such as the protocol Stack [7]. The IoV is based on the concept of Vehicular Cloud, which offers access to the Internet, and is temporarily created by interconnecting resources available on the vehicles along with Road Side Units (RSUs) [8–10]. According to ARTEMIS-project [11], the IoE is the connection of smart grids with the Internet in order to enable intelligent control of energy production, storage, and distribution. The IoS refers to the possibility of connecting sensors with the Internet using ZigBee and other

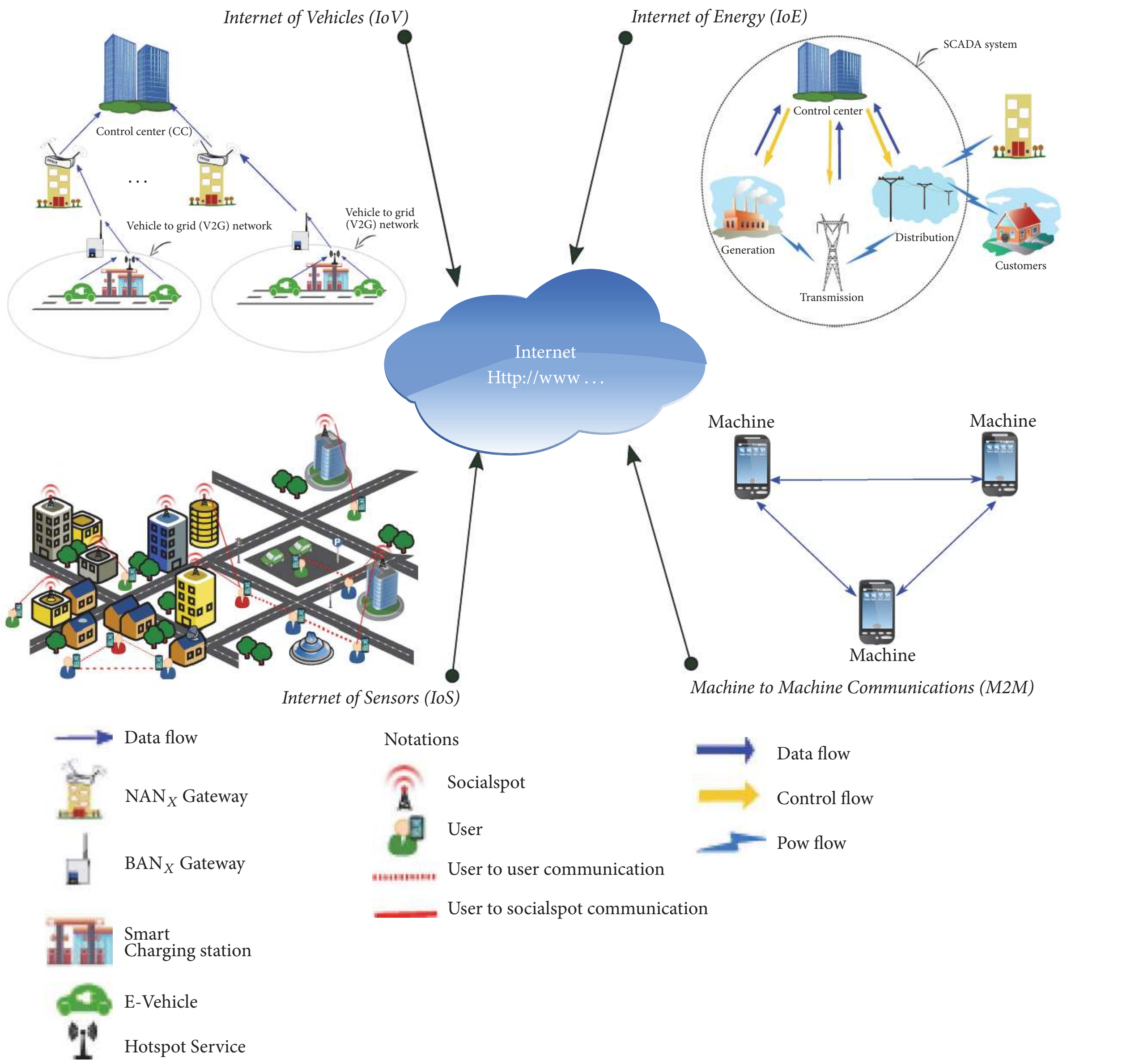


Figure 1: Internet of Things (IoT) in four environments, including: (1) Internet of Vehicles (IoV), (2) Internet of Energy (IoE), (3) Internet of Sensors (IoS), and (4) Machine to Machine Communications (M2M).

IEEE 802.15.4 based protocols [12]. The list of acronyms used in this paper is listed in Acronyms Section.

The vision of the IoT will advance based on many new features and will cope with new challenges, as shown in Figure 2, including cloud computing, M2M, IoS, IoE, IoV, social networks, software defined optical networks (SDONs), and fifth generation (5G) cellular networks. The IoT data which will be produced from billions of interactions between devices and people is going to be not only massive, but also complex and it will suffer from many security and privacy problems, especially regarding the authentication among devices. To resolve these security issues, researchers in the field of computer security have developed many authentication protocols applied in the context of the IoT. The aim of the current survey paper is to provide a comprehensive and systematic review of recent studies on published authentication protocols for the IoT in four environments, including, M2M, IoV, IoE, and IoS. More precisely more than forty authentication protocols are selected and examined in detail. The original set of papers was formed from the searchers run on SCOPUS and Web of Science from the period between 2010 and 2016. The search started on 15/10/2016 and continued until the submission date of this paper. See Table 1 for a breakdown of publication dates. The main contributions of this paper are as follows:

(i) Previous survey articles published in recent years that deal with the IoT are briefly presented.

(ii) Authentication protocols in M2M, IoV, IoE, and IoS that were evaluated under thirty-five attacks are

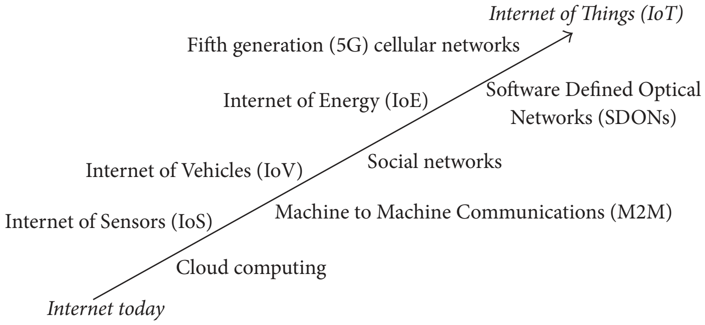

Internet of Things (IoT)
Fifth generation (5G) cellular networks
Internet of Energy (IoE)
Software Defined Optical Networks (SDONs)
Internet of Vehicles (IoV)
Social networks
Internet of Sensors (IoS)
Machine to Machine Communications (M2M)
Cloud computing
Internet today

Figure 2: Vision of the IoT with main features and challenges.

Table 1: Publication date breakdown-surveyed papers (authentication protocols).

Papers	Year
[17–24]	2010
[25–31]	2011
[32–36]	2012
[37–45]	2013
[46–51]	2014
[52–60]	2015
[61–77]	2016

discussed. Main focus is given on five attacks, which are mostly studied in earlier works, namely, man-in-the-middle attack, impersonation attack, forging attack, replay attack, and Sybil attack.

(iii) Various countermeasures and formal security verification techniques used by authentication protocols for the IoT are presented.

(iv) A side-by-side comparison in a tabular form of the current state-of-the-art of authentication protocols which are proposed for the IoT viewed from five different aspects, namely, network model, specific security goals, main processes, computation complexity, and communication overhead, is given.

(v) Open issues for M2M, IoV, IoE, and IoS are discussed.

The rest of this paper is organized as follows. Section 2 summarizes the existing survey works on different aspects of the IoT idea. In Section 3, an overview of threat models in the IoT is presented. Section 4 presents various countermeasures and formal security verification techniques. In Section 5, a taxonomy and comparison of authentication protocols for the IoT is presented. Finally, open issues and recommendations for further research are discussed in Section 6 and main conclusions are drawn in Section 7.

2. Surveys Articles for the IoT

There exist many survey articles published during recent years that deal with Internet of Things, focusing on different aspects of the IoT idea, for example, networking, applications, standardization, social interactions, security, and many more. These survey articles are categorized in terms of field of research as shown in Table 2. Internet of Things concepts attracts more and more attention as the years pass by and although a lot of different areas related to IoT are covered from previous review works, no survey article exists that thoroughly investigates authentication protocols that are especially developed for this new technology or better say this blend of technologies and systems. In this section we will briefly present all these survey articles grouped as shown in Table 2 and will discuss in more depth previous works that deal with security and privacy issues of the IoT.

The first survey article in the literature that was dealing with the IoT concept was published back in 2009 by Cooper and James [14] and focused on the challenges for database management in the IoT. Seeing the IoT from that point of view they found that the technical priorities that needed to be addressed in order to support the interconnection of every device were proper indexing, archiving, development of smart agents, the use of XML for achieving Interoperability, and novel systems that will be able to offer efficient and secure transaction management. In a later survey article that was published in 2010, Atzori et al. [6] discussed the vision of "anytime, anywhere, any media, anything" communications that the IoT would bring in our everyday lives. Based on their research author spotted two important technologies that needed to be applied in order to bring IoT into life, Internet Protocol version 6 (IPv6) and Web 2.0. The same year, the first survey article that dealt with security and privacy issues related to IoT was published [15]. In this article, Weber discussed the different measures that were needed in order to ensure the architecture's resilience to attacks, data authentication, access control, and client privacy. The article dealt with security and privacy issues from the legislation perspective mostly due to the fact that the IoT was more an idea back in 2010 than a concrete system yet. Another article dealing with security and privacy was published in 2010 from Medaglia and Serbanati [16]. The article tried to present a short term and a long-term vision of the IoT along with the security issues and solutions that would be needed.

In 2011 several published survey articles focused on the IoT [83, 87, 89, 93, 104, 126]. In [87] authors conducted a thorough analysis of the different publicly available testbeds. Bandyopadhyay and Sen [93] published an interesting survey

Table 2: Areas of research of each survey article for the IoT.

Ref.	DD	MW	AP	SE	SP	Exp	Net	ST	Arch	SR	RFID	Soc	DM	IIoT
[14, 78–80]	√													
[6, 81–84]		√												
[6, 85, 86]				√										
[87]						√								
[7, 80, 88–92]							√							
[93–98]								√						
[99–103]									√					
[104]										√				
[15, 16, 89, 90, 94, 105–119]					√									
[120, 121]											√			
[122–125]												√		
[5, 6, 90, 93, 94, 99, 126–134]			√											
[135, 136]													√	
[100]														√

DD: Data quality and database management, MW: middleware, AP: applications, SE: smart environments, SP: security and privacy, Exp: experimentation, Net: networking, ST: standardization, Arch: architecture, SR: searching, RFID: RFID technology, Soc: Social Internet of Things, DM: data mining, and IIoT: industrial Internet of Things.

article about the current developments related to IoT and the open issues back in 2011. The article managed to spot most of the challenges that IoT had and still has to face nowadays, for example, managing large amount of information and mining large volume of data, managing heterogeneity, and ensuring security privacy and trust, among others. Feasible solutions for the problem of establishing a session key between a client and a server in the context of the Internet of Things were surveyed in [89], where the authors considered the scenario where at least one peer was a sensor node. They especially focused on different cryptography solutions and how these could be applied to server and client nodes. Ma in [126] gave an overview of the objectives of the IoT and the challenges involved in IoT development while in [104] Zhang et al. covered the topic of how to build an appropriate search engine for IoT, a topic that was spotted from Cooper and James in [14] back in 2009 as a challenge to be addressed in the future.

During 2012 and 2013 the following survey articles were published [5, 82, 94–97, 99, 105, 106, 122, 123] dealing with standardization, applications, architecture, security, and privacy issues of the IoT. Articles [95–97] surveyed standardization issues and how the IETF Constrained RESTful Environments (CoRE) working group focuses on facilitating the integration of constrained devices with the Internet at the service level. These articles pointed out that all the standardized protocols are only a starting point for exploring additional open issues like resource representation, security and privacy, energy efficiency, and so on. Authors in [5, 94] gave a general overview of the current vision, applications, architectural elements, and future challenges and directions of the IoT. Miorandi et al. in [94] discussed the potential impact of the IoT on smart home automation, smart cities, environmental monitoring, health care, smart businesses, and security and surveillance making very clear, maybe for the first time, that the IoT concept involves every current or future technology that is going to be introduced in order to make our life better. Domingo in [99] performed a more narrow but extensive survey of the IoT for people with disabilities. Authors spotted the relevant application scenarios and main benefits along with the key research challenges, like customization, self-management, and security and privacy issues. They argued that as brain–computer interfaces (BCIs) are becoming commercial, they will also be a part of the IoT world. Articles [105, 106] focused on security and privacy issues as they were identified back in 2012 and 2013, respectively. Both articles agree that key management needs strong legislation, while authors in [106] take one step further and propose that grouping of the IoT devices and creating the so called intranet of things could help impose security mechanisms more effectively. Finally articles [122, 123] survey for the first time the social concept of the IoT, the so called Social Internet of Things, a concept that later will raise a lot of attraction and research works.

During 2014 and 2015 more than twenty new survey articles about IoT were published [7, 85, 98, 100, 102, 107, 108, 110, 112–116, 121, 124, 128–130, 135, 136, 212, 213]. Except articles that discussed general issues regarding IoT [98, 129, 130, 212], for example, applications, challenges, trends, and open issues, other papers focused on specific applications or research areas that are connected to the IoT idea. Authors in all three articles agree that IoT thus brings new opportunities by enabling enriched context-aware services, but it also raises new challenges that need to be addressed. Zanella et al. [85] focused specifically to an urban IoT system which is another term to describe the smart city environment. In contrast to the previous years during 2014 and 2015 a big proportion of the survey articles focus on security and privacy issues related to the IoT [107, 108, 110, 112–116], revealing the significance that security was beginning to have for cyber-physical systems. Cyber-Physical systems need to rely on IoT enabled technologies which can be effectively and efficiently supported and assisted by cloud computing infrastructures

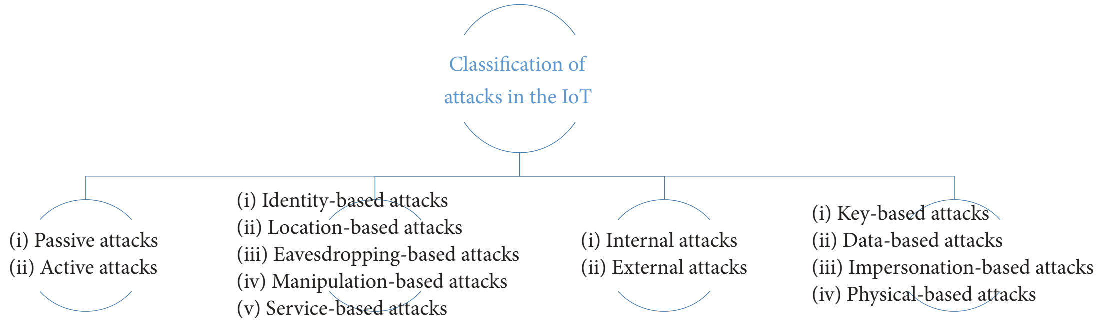

Classification of attacks in the IoT
(i) Passive attacks
(ii) Active attacks
(i) Identity-based attacks
(ii) Location-based attacks
(iii) Eavesdropping-based attacks
(iv) Manipulation-based attacks
(v) Service-based attacks
(i) Internal attacks
(ii) External attacks
(i) Key-based attacks
(ii) Data-based attacks
(iii) Impersonation-based attacks
(iv) Physical-based attacks

Figure 3: Classification of attacks in the IoT.

and platforms. The integration of IoT and cloud computing was thoroughly surveyed from Botta et al. [128] where also the possibility of exploiting fog computing capabilities for supporting the IoT concept was discussed. Data mining in the IoT context was surveyed by Tsai et al. [135] and Chen et al. [136]. Authors in [135] presented a good summary of the potentials that applying data mining technologies to the IoT could have to people, the system itself, and other interconnected systems. Authors in [136] took a step further and based on their survey and analysis proposed a big data mining system for IoT. Ortiz et al. [124] surveyed the Social Internet of Things and compared to the earlier survey articles [122, 123] proposed a generic SIoT architecture which consists of actors, a central intelligent system, an interface, and the Internet. Two articles focused on IoT-based health care technologies [121, 213], covering new platforms, applications, and security and privacy issues that arise. Authors in [100] conducted an extensive literature review about the current status and future research opportunities regarding the use of IoT in industries, the so called Industrial Internet of Things (IIoT), while in [102] authors tried to identify the impact of the Internet of Things (IoT) on Enterprise Systems in modern manufacturing.

During 2016 over fifteen new survey articles that focused on the IoT concept were published [78–80, 84, 86, 91, 103, 111, 117–119, 125, 131, 132, 134, 214]. Following the technology development three of the articles published this year focused on the integration of the cloud and the IoT, the applications, the requirements, and the security issues that arise from it [117, 131, 134]. Security was also one aspect that was covered from a number of survey articles [117–119]. Authors in [118] covered several aspects of IoT security, for example, general devices security, communication security, network security, and application, while in [119] mechanisms that reassure secure routing were investigated. In contrast to previous years, surveys published during 2016 covered new areas, such as SDN and virtualization [91], economic and pricing theory in IoT [80], social Internet of vehicles [125], and data quality [78]. Other topics covered from the survey articles were middleware [84], data models [79], mobile crowd sensing strategies [132], the deployment of IoT in smart environments [86], and the main proposed architectures for IoT [103]. Xie et al. [111] surveyed the security of the Web of Things (WoT) which is aimed to provide any electronic item (smart cards, sensors, etc.) with a URL.

Among the aforementioned surveys, the security and privacy issues that are related to the IoT were thoroughly covered and analyzed [15, 16, 89, 90, 94, 105–119]. As it is shown in Table 3 data authentication and integrity were only covered partially from He and Zeadally [121] while the rest of the articles did not cover this major security aspect. In this article we tend to survey authentication protocols for the IoT in four environments, including (1) Machine to Machine communications (M2M), (2) Internet of Vehicles (IoV), (3) Internet of Energy (IoE), and (4) Internet of Sensors (IoS). Based on this thorough analysis open issues and future directions are identified that combine both innovative research along with the application, through appropriate adaptation, of existing solutions from other fields. We believe that this study will help researchers focus on the important aspects of authentication issues in the IoT area and will guide them towards their future research.

3. Threat Models

In this section various threat models in the IoT are discussed. The summary of thirty-five attacks in M2M, IoV, IoE, and IoS and defense protocols are given in Tables 4, 5, 6, and 7, respectively. We focus on five attacks, which are mostly used by authors that propose new authentications protocols for evaluating their methods, namely, man-in-the-middle attack, impersonation attack, forging attack, replay attack, and Sybil attack. Generally, the classification of attacks [215–218] frequently mentioned in the literature is done using the following four types, as shown in Figure 3:

(1) Type A: Passive or active;

(2) Type B: Internal or external;

(3) Type C [219]: Key-based attacks, data-based attacks, impersonation-based attacks, and physical-based attacks;

(4) Type D [220]: Identity-based attacks, location-based attacks, eavesdropping-based attacks, manipulation-based attack, and service-based attacks.

3.1. Man-in-the-Middle Attack. The man-in-the-middle (MITM) attack is one of the most well known attacks in the IoT. With

Table 3: A comparison of related surveys in the literature (surveys on security and privacy for the IoT).

Survey on security and privacy for the IoT	Privacy preserving schemes	Authentication protocols	Comments
Weber (2010) [15]	0	X	Presented milestones of an adequate legal framework for IoT privacy
Medaglia and Serbanati (2010) [16]	0	X	Presented a Short-Term and Long-Term vision for IoT privacy
Roman et al. (2011) [89]	X	X	Analyzed some key management systems for sensor networks in the context of the IoT (public key cryptography and preshared keys)
Miorandi et al. (2012) [94]	0	X	Presented some security challenges in IoT, including Data confidentiality, Privacy, and Trust
Suo et al. (2012) [105]	X	X	Discussed the security requirements in each level for IoT (four key levels, i.e., recognition layer, network layer, support layer, and application layer)
Aggarwal et al. (2013) [90]	0	X	Discussed the privacy in data collection, and during data transmission and sharing
Roman et al. (2013) [106]	X	X	Presented the security issues in distributed IoT systems
Yan et al. (2014) [107]	√	X	Surveyed the privacy-preserving schemes IoT, including database query, scientific computations, intrusion detection, and data mining
Jing et al. (2014) [108]	X	X	Discussed the security issues and technical solutions in WSNs
Chabridon et al. (2014) [109]	√	X	Surveyed the state of the art of privacy technology from the perspective of the IoT
Ziegeldorf et al. [110]	√	X	Surveyed the privacy threats and challenges in the IoT
Keoh et al. (2014) [112]	X	X	Presented an overview of the efforts in the IETF to standardize security solutions for the IoT ecosystem
Sicari et al. (2015) [113]	0	X	Discussed the privacy, trust, enforcement, secure middleware, and mobile security in the IoT
Granjal et al. (2015) [114]	X	0	Discussed IoT communications and security at the physical and MAC layers
Sadeghi et al. (2015) [115]	X	X	Discussed an introduction to Industrial IoT systems with the related security and privacy challenges
Nguyen et al. (2015) [116]	0	X	Surveyed the secure communication protocols for the IoT, including asymmetric key schemes and symmetric key predistribution schemes
He and Zeadally (2015) [121]	X	0	Analyzed only the RFID authentication schemes for the IoT in healthcare environment using elliptic curve cryptography
Xie et al. (2016) [111]	X	X	Reviewed the security issues for Web of Things
Singh et al. (2016) [117]	X	X	Analyzed the state of cloud-supported IoT to make explicit the security considerations
Li et al. (2016) [118]	X	X	Analyzed the security requirements and potential threats in a four-layer architecture for the IoT
Airehrour et al. (2016) [119]	X	X	Analyzed the security of routing protocols for the IoT
Our work	0	√	Surveyed the authentication protocols for the IoT in four environments, including (1) Machine to Machine Communications (M2M), (2) Internet of Vehicles (IoV), (3) Internet of Energy (IoE), and (4) Internet of Sensors (IoS)

√ indicates fully supported; X indicates not supported; 0 indicates partially supported.

Table 4: Summary of attacks in Machine to Machine Communications (M2M) and defense protocols.

Adversary model	Authentication protocols for M2M								
	[62]	[61]	[46]	[38]	[34]	[53]	[47]	[137]	[37]
Audio replay attack	√	0	X	0	0	0	X	X	0
Changing distance attack	√	X	X	X	X	X	X	X	X
Same-type-device attack	√	X	X	X	X	X	X	X	X
Composition attack	√	X	X	X	X	X	X	X	X
Redirection attack	0	√	0	√	X	X	0	X	√
Man-in-the-middle attack	0	√	0	√	0	0	X	X	√
Substitution attack	0	0	0	0	0	X	X	X	X
DoS attack	X	√	X	√	X	X	√	X	X
Replay attack	0	X	X	√	0	√	X	X	√
Forging attack	X	X	X	0	X	X	X	X	X
Colluding attack	0	X	X	0	X	X	0	X	X
Flooding attack	0	X	X	X	X	X	0	X	0
Side-channel attack	0	X	X	X	X	X	0	X	0
False messages attack	0	X	X	X	0	0	0	X	0
Sybil attack	X	X	X	X	0	0	X	X	0
Movement tracking	X	X	X	X	0	X	X	X	0
Message modification	X	X	X	X	0	X	X	X	X
Impersonation attack	X	X	X	X	0	√	√	X	X
Guessing attack	X	X	X	X	X	√	X	X	X
Stolen-verifier attack	X	X	X	X	X	√	X	X	X
Wormhole attack	0	0	X	0	X	0	X	X	0
Blackhole attack	0	0	X	0	0	0	X	X	0
Attribute-trace attack	X	X	X	X	0	X	X	X	X
Eavesdropping attack	X	X	X	X	0	0	X	X	0
Chosen-plaintext attack	X	X	X	X	0	X	X	X	0
Spam attack	0	X	X	X	0	0	X	X	0
Identity theft attack	0	X	X	X	X	0	X	X	X
User manipulation attack	0	X	X	X	X	0	0	X	0
Routing attack	0	X	X	X	X	0	X	X	X
Linkability attack	0	X	X	X	X	X	X	X	X
Rejection attack	X	X	X	X	X	X	X	X	X
Successive-response attack	X	X	X	X	X	X	X	X	X
Packet analysis attack	X	0	X	X	X	0	X	X	0
Packet tracing attack	X	0	X	X	X	0	X	X	0
Brute-force attack	0	0	X	0	0	X	0	0	X

√ indicates fully supported; X indicates not supported; 0 indicates partially supported.

MITM attack, an adversary can spoof the identities of two honest nodes ($N1$ and $N2$) involved in a network exchange and pass $N1$ for $N2$ and vice versa, that is, taking control of the communication channel between $N1$ and $N2$. Under this control, an adversary can intercept, modify, change, or replace target victims' communication traffic. However, we note here that there is a good survey article published in 2016 by Conti et al. in [13], which presents a comprehensive survey on MITM attacks. Specifically, authors in [13] classify MITM attacks in three different categories, namely, (1) MITM based on impersonation techniques, (2) MITM based on the communication channel, and (3) MITM based on the location of an adversary. As presented in Figure 4, at any moment an adversary can set up a connection between False BTS and Legitimate MS, where False MS impersonates the victim's MS to the real network by resending the identity information. Moreover, as presented in Table 8, there are twelve authentication protocols for the IoT, which can detect and avoid the MITM attack. The four authentication protocols in [61, 75, 77, 146] use the idea of mutual authentication. The two authentication protocols [37, 38] use the idea of authentication acknowledgement phase. With the protocol [139], all packets are fully encrypted with the receiver's public key, which can prevent the MITM attack. On the other hand, with the protocol [39], when the keys generated at the mobile router and the relay router for authentication are based on

Table 5: Summary of attacks in Internet of Vehicles (IoV) and defense protocols.

Adversary model	Authentication protocols for IoV								
	[39]	[40]	[63]	[64]	[65]	[66]	[48]	[52]	[54]
Audio replay attack	0	0	0	X	0	0	X	0	X
Changing distance attack	X	X	X	X	X	X	X	X	X
Same-type-device attack	X	X	X	X	X	X	X	X	X
Composition attack	X	X	X	X	X	X	X	X	X
Redirection attack	0	0	X	X	X	X	X	X	X
Man-in-the-middle attack	√	0	0	X	X	√	0	X	X
Substitution attack	0	0	0	X	X	0	√	X	X
DoS attack	√	X	X	√	√	√	X	X	X
Replay attack	√	√	√	X	0	0	0	√	0
Forging attack	0	√	X	X	X	0	X	X	X
Colluding attack	0	√	X	0	X	X	X	X	X
Flooding attack	X	X	X	0	X	X	X	X	X
Side-channel attack	X	X	X	0	√	X	X	X	X
False messages attack	X	X	X	X	√	X	X	X	0
Sybil attack	0	X	X	X	√	0	X	X	0
Movement tracking	X	X	X	X	X	X	X	√	X
Message modification	X	X	X	X	X	X	0	√	X
Impersonation attack	X	X	X	X	X	√	X	0	X
Guessing attack	X	X	X	X	X	X	X	X	0
Stolen-verifier attack	X	X	X	X	X	X	X	X	0
Wormhole attack	0	0	X	X	0	X	0	0	0
Blackhole attack	0	0	X	X	0	X	0	0	0
Attribute-trace attack	X	X	X	X	X	0	X	X	0
Eavesdropping attack	X	X	0	0	0	X	X	0	0
Chosen-plaintext attack	X	X	X	0	X	X	0	X	0
Spam attack	X	X	X	0	X	0	0	X	X
Identity theft attack	X	X	X	0	X	X	0	X	X
User manipulation attack	X	X	X	0	X	X	0	0	X
Routing attack	0	X	0	X	0	X	0	0	0
Linkability attack	X	X	X	X	X	0	X	0	X
Rejection attack	X	X	X	X	X	0	X	0	0
Successive-response attack	X	X	X	X	X	0	X	X	X
Packet analysis attack	0	0	X	X	0	0	X	0	0
Packet tracing attack	0	0	X	X	0	0	X	0	0
Brute-force attack	X	X	X	X	X	0	X	0	0

√ indicates fully supported; X: indicates not supported; 0: indicates partially supported.

the concept of symmetric polynomials, an adversary can not identify a shared key between two legitimate users making it impossible for him to impersonate a mobile router or a relay router. In addition, both protocols [72, 142] are based on a password and biometric update phase in order to prevent an adversary from impersonating the passwords of a smart meter.

3.2. Impersonation and Forging Attack. Under the impersonation and forging attack in the IoS, an adversary can eavesdrop or intercept the login request message of previous sessions over the public/open channel during authentication protocol execution. After that, he can modify and retransmit the message to the user in order to impersonate as a valid user, as defined by Amin and Biswas [70] and shown in the Figure 5. We note that this attack is analyzed more in authentication protocols that are produced for the IoS. Moreover, as presented in Table 9 there are sixteen authentication protocols for the IoT, which can detect the impersonation and forging attack. The protocol [40] uses two ideas, namely, (1) linear search algorithm and (2) binary search algorithm. The protocol [47] uses strong anonymous access authentication and user tracking on a disputed access request, to prevent the impersonation and forging attack. Besides, the idea of using a password for detecting the impersonation of the gateway node is presented by four authentication protocols

Table 6: Summary of attacks in Internet of Energy (IoE) and defense protocols.

Adversary model	Authentication protocols for IoE								
	[28]	[49]	[138]	[139]	[140]	[141]	[142]	[55]	[67]
Audio replay attack	X	X	X	X	X	X	X	X	X
Changing distance attack	0	X	X	X	X	0	0	0	X
Same-type-device attack	X	X	X	0	X	X	X	X	X
Composition attack	X	X	X	X	X	X	X	X	X
Redirection attack	X	X	X	0	X	0	X	X	X
Man-in-the-middle attack	0	0	0	√	0	0	√	0	0
Substitution attack	X	0	X	X	X	X	0	0	X
DoS attack	X	X	0	√	X	0	√	X	0
Replay attack	0	√	0	√	√	√	√	0	√
Forging attack	√	0	0	0	0	X	X	X	X
Colluding attack	X	0	X	0	0	X	0	0	X
Flooding attack	X	0	X	0	X	X	0	0	0
Side-channel attack	X	X	X	X	X	0	0	0	X
False messages attack	0	√	0	0	0	0	0	0	√
Sybil attack	0	0	0	0	0	0	X	X	0
Movement tracking	0	X	X	X	X	0	X	X	0
Message modification	0	√	0	0	0	0	0	0	√
Impersonation attack	0	0	X	X	0	X	0	0	0
Guessing attack	X	0	X	0	X	X	X	X	X
Stolen-verifier attack	X	X	X	X	X	X	X	X	X
Wormhole attack	X	X	0	X	X	0	0	0	0
Blackhole attack	X	X	0	X	X	0	0	0	0
Attribute-trace attack	X	X	X	0	X	0	X	X	X
Eavesdropping attack	0	0	0	0	0	0	0	0	0
Chosen-plaintext attack	X	X	X	0	X	√	X	X	X
Spam attack	X	X	X	0	X	X	X	X	X
Identity theft attack	X	X	0	0	0	X	0	0	0
User manipulation attack	X	X	X	X	0	X	X	X	0
Routing attack	X	X	0	0	X	X	X	X	X
Linkability attack	0	X	0	0	X	X	0	0	X
Rejection attack	0	X	0	0	0	X	0	0	0
Successive-response attack	0	X	X	0	X	X	X	X	0
Packet analysis attack	0	√	0	0	0	X	0	0	√
Packet tracing attack	0	0	X	0	0	0	0	0	0
Brute-force attack	X	X	X	√	X	X	√	0	X

√ indicates fully supported; X indicates not supported; 0 indicates partially supported.

[53, 77, 147, 148]. In addition, the hash mechanism which is applied on the shared key between gateway wireless node and sensors can prevent the impersonation of a sensor.

3.3. Replay Attack. The replay attacks are MITM attacks, which consist of intercepting data packets and retransmitting them as is (without any decryption) to the destination server, as shown in Figure 6 (intercepting *D*3 and retransmitting it). Under this attack, an adversary can obtain the same rights as the user. A wormhole attack can be launched through the replay attack as shown in Figure 7. However, there are twenty-four authentication protocols for the IoT, which can detect and avoid the replay attack, as presented in Table 10. These authentication protocols use three ideas, namely, Timestamp, Hash function, and random numbers. The idea of random numbers is used by [37–39, 53]. The idea of hash function is used by protocols [49, 143], such as the IPSec protocol which implements an antireplay mechanism based on message authentication code (MAC) [221]. In addition, the idea of Timestamp in the encrypted messages is used by [40, 49, 52, 63, 67, 68, 70, 72, 73, 75–77, 139–144, 148].

3.4. Sybil Attack. With the Sybil attack, a malicious node can claim different identities in order to gain an advantage over legitimate nodes, as shown in Figure 8. Based on the member secrets generation stage, Zhang et al. [65] proposed

Table 7: Summary of attacks in Internet of Sensors (IoS) and defense protocols.

Adversary model	Authentication protocols for IoS															
	[68]	[69]	[143]	[70]	[71]	[72]	[73]	[74]	[75]	[144]	[76]	[145]	[77]	[146]	[147]	[148]
Audio replay attack	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Changing distance attack	0	X	0	X	X	X	X	X	X	X	X	X	X	X	X	X
Same-type-device attack	0	X	0	X	X	X	X	X	0	X	X	X	X	X	X	X
Composition attack	√	0	X	X	0	0	X	0	0	X	X	X	0	0	0	0
Redirection attack	√	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0
Man-in-the-middle attack	0	0	0	0	0	√	0	0	√	0	0	0	√	√	√	0
Substitution attack	0	X	X	X	X	X	0	X	0	0	0	0	0	X	X	X
DoS attack	0	0	0	X	0	X	0	X	√	0	0	X	0	0	0	0
Replay attack	√	0	√	√	0	√	√	0	√	√	√	X	√	0	0	√
Forging attack	0	√	0	X	0	√	0	0	0	0	0	X	0	√	√	0
Colluding attack	0	0	0	X	0	0	0	X	0	0	0	√	0	0	0	0
Flooding attack	√	0	X	X	0	0	0	X	0	0	0	0	0	0	0	0
Side-channel attack	X	0	X	X	X	X	X	X	X	X	X	X	0	X	X	X
False messages attack	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sybil attack	0	0	√	0	X	X	X	0	0	0	0	0	0	0	0	0
Movement tracking	0	0	X	X	0	X	X	0	0	0	0	0	0	0	0	0
Message modification	0	0	0	0	0	0	0	√	0	0	0	0	√	0	0	0
Impersonation attack	√	√	0	√	√	0	0	√	0	√	√	X	√	0	0	√
Guessing attack	√	√	0	√	0	0	0	0	0	√	√	X	√	0	√	0
Stolen-verifier attack	√	X	X	0	0	X	X	X	√	0	0	0	√	0	0	0
Wormhole attack	0	0	0	0	0	0	0	X	X	X	X	X	0	X	X	X
Blackhole attack	0	0	0	0	0	0	0	X	X	X	X	X	0	X	X	X
Attribute-trace attack	X	X	X	X	X	0	X	X	0	X	X	X	0	X	X	X
Eavesdropping attack	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0
Chosen-plaintext attack	X	X	X	X	X	X	X	X	X	X	X	X	X	0	0	0
Spam attack	X	X	X	0	X	X	0	X	0	X	X	X	X	0	0	0
Identity theft attack	0	0	0	X	X	X	0	X	0	X	X	X	0	0	0	0
User manipulation attack	0	0	X	0	0	X	0	0	0	0	0	0	0	0	0	0
Routing attack	0	0	0	0	0	X	0	X	0	X	X	X	0	X	X	X
Linkability attack	0	0	0	0	0	0	0	X	0	X	X	X	0	X	X	X
Rejection attack	0	0	0	0	0	X	0	X	0	X	X	X	0	X	X	X
Successive-response attack	√	X	0	X	0	X	X	X	0	X	X	X	X	X	X	X
Packet analysis attack	0	0	X	0	0	X	X	√	X	X	X	X	X	0	0	0
Packet tracing attack	0	0	X	0	√	X	X	√	X	X	X	X	X	0	0	0
Brute-force attack	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

√ indicates fully supported; X indicates not supported; 0 indicates partially supported.

a distributed aggregate privacy-preserving authentication protocol, called DAPPA, which is robust and resilient to the Sybil attacks in the IoV environment. Using a token-based authentication approach, Jan et al. [143] proposed a payload-based mutual authentication protocol, called PAWN in the IoS environment. PAWN can detect the Sybil attacks based on the cluster formation between neighboring nodes and their nearest cluster head.

4. Countermeasures and Formal Security Verification Techniques

In order to satisfy the authentication model to secure IoT, namely, mutual authentication, perfect forward secrecy, anonymity, and untraceability, the authentication protocols use both cryptosystems and non-cryptosystems countermeasures. Tables 11, 12, 13, and 14 present the cryptosystems and countermeasures used in authentication protocols for M2M, IoV, IoE, and IoS, respectively. In this section, we will discuss the countermeasures and present the formal security verification techniques used in these authentication protocols for the IoT.

4.1. Countermeasures. Based on the cryptosystems, the existing authentication protocols for the IoT can mainly be classified into three categories: symmetric-cryptosystem based, asymmetric-cryptosystem-based, and hybrid protocols, as shown in Figure 9. As presented in the following (Tables 11,

Table 8: Approaches for detecting and avoiding the man-in-the-middle attack.

Protocol	Data attacked	Approach
Lai et al. (2016) [61]	Communication channel between the mobile management entity and the home subscriber server	Mutual authentication and key agreement between multiple M2M devices and the core network simultaneously
Lai et al. (2013) [38]	The data between the mobiles equipment's and the 3GPP network	Authentication acknowledge phase
Cespedes et al. (2013) [39]	(i) Identify a shared key between two legitimate users (ii) Impersonate a mobile router or a relay router	The keys generated at the mobile router and the relay router for authentication are based on the concept of symmetric polynomials
Dolev et al. (2016) [66]	Communication channel between the vehicles	(i) Twofold authentication (ii) Periodic certificate restore
Nicanfar et al. (2011) [139]	(i) Communication channel between the smart meter and the authentication agent (ii) Communication channel between the authentication agent and the security associate (SA) server	All packets are fully encrypted with the receivers public key
Nicanfar et al. (2014) [142]	The passwords of smart meter	Changing the server password more often
Das (2016) [72]	The login request message during the login phase	Password and biometric update phase
Lai et al. (2013) [37]	Can occur while connecting to a base station	Authentication acknowledge phase
Farash et al. (2016) [75]	Data between the sensor node, users, and gateway node	Mutual authentication
Jiang et al. (2017) [77]	Data between the Sensor node, users and Gateway node	Mutual authentication
Wu et al. (2016) [146]	Data between the Sensor node, users and Gateway node	Mutual authentication
Das et al. (2016) [147]	The lost/stolen smart card of a legal user	Password change phase

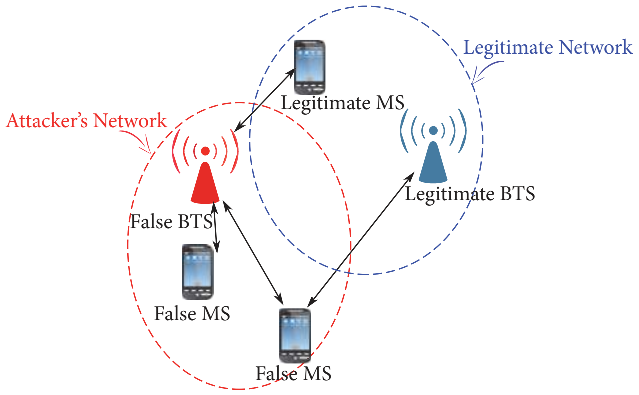


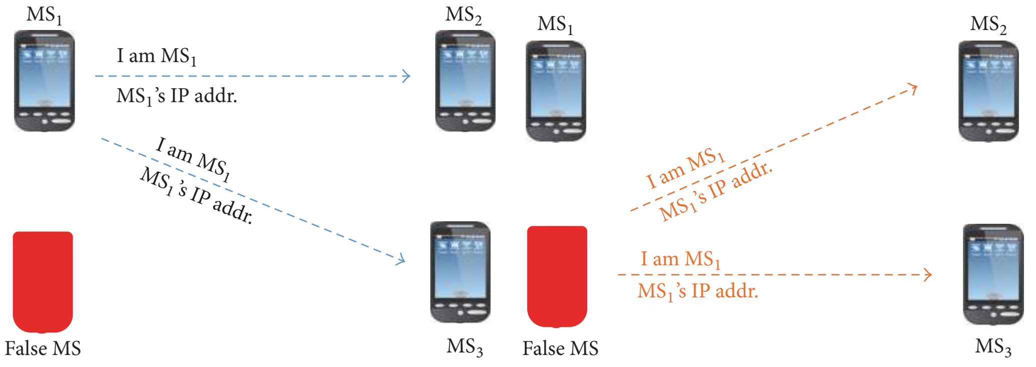
Figure 4: MITM attack on GSM as defined by Conti et al. in [13], BTS: Base Transceiver Station; MS: Mobile Station.

12, 13, and 14), most authentication protocols use a secure cryptographic hash function [149].

As presented in Table 11, the protocol [137] uses three cryptosystems, namely, original data acquisition, spatial-domain transformation, and time-domain transformation. The protocol [62] use two matching algorithms, namely, correlation coefficient-based matching algorithm (C-MA) and deviation ratio-based matching algorithm (D-MA). The aggregate message authentication codes (AMACs) [150] are used by both schemes [37, 61]. The AMAC tool is a tuple of the following probabilistic polynomial time algorithms: *Authentication algorithm*, *Aggregation algorithm*, and *Verification algorithm*. The authentication algorithm outputs a *tag* tag, where the aggregate of tags can be simply computing the XOR of all the tag values; that is, $tag = tag_1 \oplus tag_2 \oplus \cdots \oplus tag_l$, where $1, \ldots, l$ are identifiers. The protocol [46] uses certificateless aggregate signature [151], which enables an algorithm to aggregate n signatures of n distinct messages from n users into a single short signature. In addition, the certificateless aggregate signature scheme is secure against existential forgery in the chosen aggregate model. The aggregate signature generator computes $V = \sum_{i=1}^{n} V_i$ and outputs $\sigma_n = (U_1, \ldots, U_n, V)$ as an aggregate signature. The protocol [38] uses Elliptic Curve Diffie-Hellman (ECDH) [152], which is an anonymous key agreement protocol. The protocol [34] uses ID-based signature scheme [153] that consists of four algorithms, *Setup*, *Extract*, *Sign*, and *Verify*. With *Setup* algorithm, the trust authority chooses efficiently computable monomorphisms. The trust authority performs the *Extract* algorithm when a signer requests the secret key corresponding to their identity. The *Sign* algorithm produces a signature from the user with identity *ID* on the message *m*. Therefore, the protocol [53] uses advanced encryption standard (AES) [154], which is a symmetric encryption standard intended to replace the Data Encryption Standard (DES) [222] that has become too weak in view of current attacks. The protocol [47] uses the Linear Combination Encryption (LCE) [155], which is an extension of ElGamal encryption [223] that is secure in groups where the Decision Diffie-Hellman (DDH) problem is easy but the Computational Diffie-Hellman (CDH) problem is hard. With the LCE scheme [155], a user's public and secret keys are defined as $pk = (u, v, w_1 = u^x, w_2 = v^y)$ and $sk = (x, y)$,

Table 9: Approaches for detecting and avoiding the impersonation and forging attack.

Protocol	Data attacked	Approach
Wasef and Shen (2013) [40]	Forge the revocation check	(i) Linear search algorithm (ii) Binary search algorithm
Chung et al. (2016) [69]	Impersonate the mobile node	Login and authentication phase
Das (2016) [72]	Eavesdrop or intercept the login request message of the previous sessions	Authentication and key agreement phase
Wu et al. (2016) [146]	The data produced by the smart card in the Login phase	Elliptic curve cryptosystem
Das et al. (2016) [147]	Eavesdrop, modify, or delete the contents of the transmitted messages	Password and biometric update
Sun et al. (2015) [53]	Information leakage of the M2M server	The authentication process based on password
Lai et al. (2014) [47]	Forge and/or modify the authentication messages	(i) Strong anonymous access authentication (ii) User tracking on a disputed access request
Dolev et al. (2016) [66]	Forge and/or modify the authentication messages	Two rounds of session key
Kumari et al. (2016) [68]	Impersonation of user and sensor node	Gateway wireless node does not maintain any record to store user-specific information
Amin and Biswas (2016) [70]	Intercepts the login request message	Authentication and key agreement
Gope and Hwang (2016) [71]	The server's secret key	Adversary has no knowledge about the secret identity of the gateway
Jiang et al. (2016) [74]	Gets the user smart card	The hash mechanism using the shared key between gateway wireless node and sensor
Srinivas et al. (2017) [144]	Impersonation of the gateway node	Noninvertible cryptographic one way hash function property
Kumari et al. (2016) [76]	Impersonation of the gateway node	Secret session key
Jiang et al. (2017) [77]	Gets the user smart card	Password
Liu and Chung (2016) [148]	Intercepts the login request message	Password



(a) Before the impersonation attack

(b) After the impersonation attack

Figure 5: Impersonation attack, MS: Mobile Station.

where $u, v \leftarrow G_1$ and $x, y \leftarrow Z_p^*$. The message M is encrypted to $(D_1 = u^a, D_2 = v^b, D_3 = M \cdot w_1^a w_2^b)$ where $a, b \in Z_p^*$ are random. Then, the original message M is decrypted from the ciphertext (D_1, D_2, D_3) by $D_3 \cdot (D_1^x \cdot D_2^y)^{-1}$.

As presented in Table 12, the protocol [39] uses both countermeasures, namely, Proxy Mobile IP (PMIP) [156] and Symmetric Polynomials [157]. The PMIP is a localized network based IP mobility protocol (RFC 5213 [224]) that defines two entities: the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA). The symmetric polynomial is defined as any polynomial of two or more variables that achieves the interchangeability property, that is, $f(x, y) = f(y, x)$. For example, given two users identities 1

Table 10: Approaches for detecting and avoiding the replay attack.

Protocol	Data attacked	Approach
Lai et al. (2013) [38]	Replaying the data between the mobiles equipment and the 3GPP network	Random numbers
Sun et al. (2015) [53]	Replaying the intercepted login message	Random numbers
Lai et al. (2013) [37]	Replaying the message between serving gateway and home subscriber server	Random numbers
Cespedes et al. (2013) [39]	Replaying one of the router solicitation messages	Random numbers
Wasef and Shen (2013) [40]	Replaying the disseminated messages in IoV	Timestamp
Shao et al. (2016) [63]	Replaying the disseminated messages in IoV	Timestamp
Zhang et al. (2016) [52]	Replaying the disseminated messages in IoV	Timestamp
Li et al. (2014) [49]	Replaying the electricity consumption reports	Merkle hash tree technique
Nicanfar et al. (2011) [139]	Replaying the electricity consumption reports	Timestamp
Chim et al. (2011) [140]	Replaying the electricity consumption reports	Timestamp
Fouda et al. (2011) [141]	Replaying the electricity consumption reports	Timestamp
Nicanfar et al. (2014) [142]	Forwarding a previous acknowledgment from the smart meter to the server	Timestamp
Mahmood et al. (2016) [67]	Intercept messages by home area network and replay those archaic messages to building area network gateway	Timestamp
Kumari et al. (2016) [68]	Intercept and replay the login request to gateway wireless node	Timestamp
Jan et al. (2016) [143]	Eavesdrop on advertisement packets and/or join-request packets and replay in other parts of the network	Hash function and ring keys
Amin and Biswas (2016) [70]	Replaying the message in the IoS	Timestamp
Das (2016) [72]	Replaying the login request message	Timestamp
Chang and Le (2016) [73]	Replaying the login request message	Timestamp
Farash et al. (2016) [75]	Replaying the login request message	Timestamp
Srinivas et al. (2017) [144]	Replaying the messages in the IoS	Timestamp
Kumari et al. (2016) [76]	Intercept and replay the login request to gateway wireless node	Timestamp
Jiang et al. (2017) [77]	Intercept the login request	Timestamp
Liu and Chung [148]	Intercept the login request	Timestamp

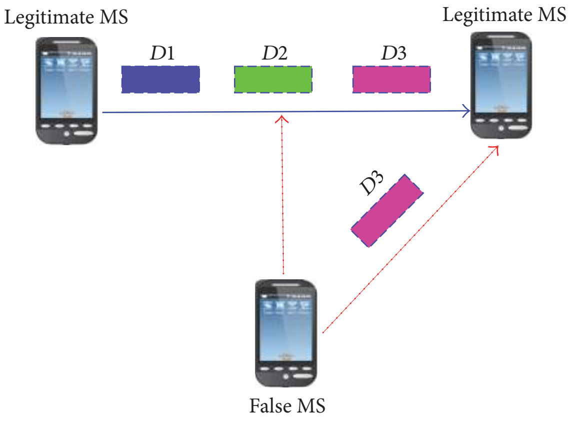


Figure 6: Replay attack, MS: Mobile Station.

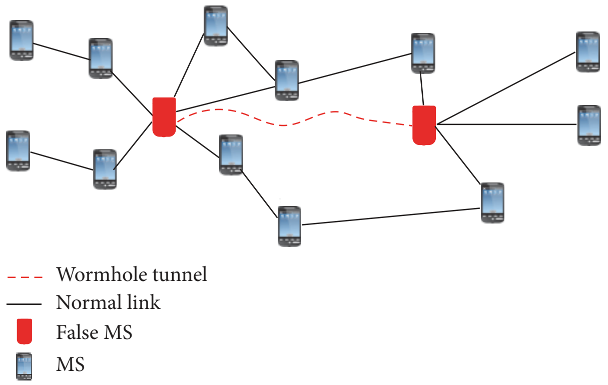


Figure 7: Wormhole attack.

and 2, and the symmetric polynomial $f(x, y) = x^2 y^2 + xy + 10$, the resultant evaluation functions are $f(1, y) = y^2 + y + 10$ and $f(2, y) = 4y^2 + 2y + 10$, respectively. Then, if user 1 evaluates its function $f(1, y)$ for user 2, it obtains $f(1, 2) = 16$. In the same way, $f(2, y)$ for user 1, user 2 obtains $f(1, 2) = 16$. As a result, both users share a secret key, 16, without transmitting any additional messages to each other. Contrary to this idea of symmetric polynomials, the protocol [40] uses the idea of search algorithms [158], which include nonoptimized search algorithms, such as linear search algorithm, and optimized search algorithms such as binary search algorithm, and lookup hash tables. In another work [159] Chaum and van Heyst introduce the idea of group signatures in order to

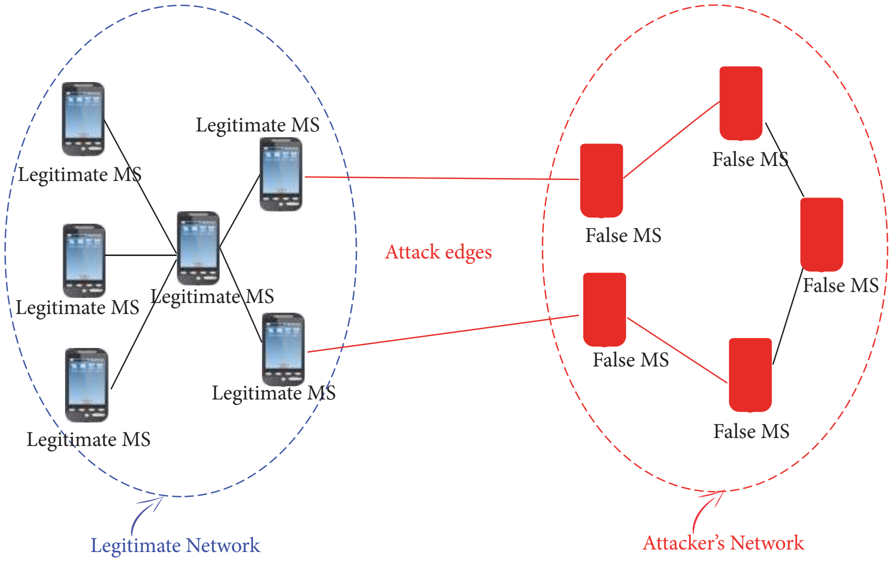


Figure 8: Sybil attack, MS: Mobile Station.

provide anonymity for signers. The protocol [63] uses this idea based on the Strong Diffie-Hellman assumption and the Decision Linear assumption. The protocol [64] uses three countermeasures, namely, (1) Merkle Hash Tree (MHT) [161], (2) TESLA scheme [162], and (3) Elliptic Curve Digital Signature Algorithm (ECDSA) [163]. The MHT is a binary tree structure where each leaf is assigned a hash value and an inner node is assigned the hash value of its children. To achieve source authentication, the TESLA scheme uses one-way hash chains with the delayed disclosure of keys based on symmetric cryptography. The protocol [65] uses multiplicative secret sharing technique [164] where the user can generate one-time pseudonym private key pairs and leakage-resilient locally. Similar to the protocol [63], the protocol [66] uses the idea of digital signatures [167]. The protocol [48] uses keyed-hashing for message authentication (HMAC) [169] to instantiate the pseudorandom function in the prototype implementation of electric vehicle ecosystem. The protocol [52] uses two similar ideas, namely, identity-based public key cryptosystem [165] and identity-based aggregate signature [166]. For providing a flexible attribute management, the protocol [54] uses an anonymous attribute-based group setup scheme [168] that incorporates the policy-based data access control in the ciphertext.

As presented in Table 13, the protocol [28] uses two types of verification, namely, Heavy signing light verification (HSLV) and Light signing heavy verification (LSHV), which is based on the HORS scheme [170]. The HSLV uses the following three algorithms: *Key Generation*, *Signing*, and *Verification*. The *Key Generation* algorithm outputs the public key $PK = (k, v_1, v_2, \dots, v_t)$ and the secret key $SK = (k, s_1, s_2, \dots, s_t)$ where the trusted authority generates t random l-bit strings $s_1, s_2, \dots, s_t$. The signature is $(c, (s_{i1}, s_{i2}, \dots, s_k))$ generated by the *Signing* algorithm. To verify a signature $(c', (s'_{i1}, s'_{i2}, \dots, s'_k))$ over message m, the user check if the output integers $i1 > i2 > ik$ and $f(s'_j) = v_{ij}$ hold. On the other hand, with LSHV, the signature verification process verifies the k elements of a signature by applying the one-way function for a distinct number of times over each element. Similar to the protocol [64], the protocol [49] uses the same idea of Merkle Hash tree technique [171]. In order to increase the level of security, the protocol [138] uses three cryptosystems, namely, short signatures (BLS) [172], batch verification [173], and signature aggregation [174]. The BLS is introduced by Boneh-Lynn-Shacham [172], which is based on Gap Diffie-Hellman groups. Specifically, the BLS scheme uses the following three algorithms: (1) *Key generation* algorithm to output the public key $v \in G_2$ and the private key x, where $x \leftarrow Z_p$ and $v \leftarrow {g_2}^x$; (2) *Signing* algorithm to generate a signature $\sigma \in G_1$, where $\sigma \leftarrow h^x$ and $h \leftarrow H(M) \in G_1$; and (3) *Verification* algorithm to verify that (g_2, v, h, σ) is a valid co-Diffie-Hellman tuple. The author of short signatures (BLS) [172], that is, Boneh et al., proposes the idea of signature aggregation [174], where an aggregate signature is valid only if it is an aggregation of signatures on distinct messages. Similar to the protocol [39], the protocol [139] uses the same cryptosystem, that is, identity-based public key cryptosystem [165]. Therefore, both protocols [55, 140] use the two same cryptosystems, namely, (1) the public key encryption, such as RSA [175], and (2) HMAC, such as SHA-1 [176] and MD5 [177]. The protocol [141] uses the Diffie-Hellman key establishment protocol [178] in order to provide forward secrecy in Transport Layer Security's ephemeral modes. The protocol [142] uses the EIBC mechanism [179], which is based on the original model developed by Boneh and Franklin. In addition, the protocol [55] uses the Homomorphic Encryption [181] and the Bloom Filter [182]. The protocol [67] uses two cryptosystems, (1) HMAC, such as SHA-1 [176] and MD5 [177], and (2) a symmetric encryption/decryption algorithm [178]. As presented in Table 14, the protocol [68] uses two countermeasures, namely, Chebyshev Chaotic Maps [183] and Semigroup Property of Chebyshev Polynomials

Table 11: Cryptosystems and Countermeasures used in authentication protocols for Machine to Machine Communications (M2M).

Cryptosystems and countermeasures	Authentication protocols for M2M								
	[62]	[61]	[46]	[38]	[34]	[53]	[47]	[137]	[37]
Secure cryptographic hash function [149]		√	√	√	√	√		√	√
Original data acquisition								√	
Spatial-Domain transformation								√	
Time-domain transformation								√	
Correlation coefficient-based matching algorithm (C-MA)	√								
Deviation ratio-based matching algorithm (D-MA)	√								
Aggregate message authentication codes (AMACs) [150]		√							√
Certificateless aggregate signature [151]			√						
Elliptic Curve Diffie-Hellman (ECDH) [152]				√					
ID-based signature scheme [153]					√				
Advanced encryption standard (AES) [154]						√			
Hybrid Linear Combination Encryption [155]							√		

Table 12: Cryptosystems and countermeasures used in Authentication protocols for Internet of Vehicles (IoV).

Cryptosystems and countermeasures	Authentication protocols for IoV								
	[39]	[40]	[63]	[64]	[65]	[66]	[48]	[52]	[54]
Secure cryptographic hash function [149]		√	√	√	√	√		√	√
Proxy Mobile IP (PMIP) [156]	√								
Symmetric polynomials [157]	√								
Search algorithms [158]		√							
Group signature [159, 160]			√						
Merkle hash tree (MHT) [161]				√					
TESLA scheme [162]				√					
ECDSA signature [163]				√					
Multiplicative secret sharing technique [164]					√				
Identity-based public key cryptosystem [165]								√	
Identity-based aggregate signature [166]								√	
Digital signatures [167]						√			
Anonymous attribute-based group setup scheme [168]									√
Keyed-hashing for message authentication (HMAC) [169]							√		

Table 13: Cryptosystems and countermeasures used in authentication protocols for Internet of Energy (IoE).

Cryptosystems and countermeasures	Authentication protocols for IoE								
	[28]	[49]	[138]	[139]	[140]	[141]	[142]	[55]	[67]
Secure cryptographic hash function [149]	√		√			√	√		
HORS scheme [170]	√								
Heavy signing light verification (HSLV) [170]	√								
Light signing heavy verification (LSHV) [170]	√								
Merkle Hash tree technique [171]		√							
Short signatures (BLS) [172]			√						
Batch verification [173]			√						
Signature aggregation [174]			√						
Identity-based public key cryptosystem [165]				√					
Public-key encryption, such as RSA [175]					√			√	
HMAC, such as SHA-1 [176] and MD5 [177]					√			√	√
Diffie-Hellman key establishment protocol [178]						√			
EIBC mechanism [179]							√		
ID-based cryptography (IBC) [180]							√		
Digital signatures [167]								√	
Homomorphic encryption [181]								√	
Bloom filter [182]								√	
Commitment scheme								√	
Symmetric encryption/decryption algorithm [178]									√

Table 14: Cryptosystems and countermeasures used in authentication protocols for Internet of Sensors (IoS).

Cryptosystems and countermeasures	Authentication protocols for IoS													
	[68]	[69]	[143]	[70]	[71]	[72]	[73]	[74]	[75]	[144]	[76]	[145]	[77]	[146]
Secure cryptographic hash function [149]	√	√	√	√	√	√	√	√	√	√	√	√	√	
Chebyshev chaotic maps [183]	√													
Chebyshev polynomials [184]	√													
ID-based cryptography (IBC) [180]		√		√	√									
Advanced encryption standard (AES) [185]			√											
Biometric						√								
Password						√				√	√			
Smart card						√	√	√	√	√	√			
Fuzzy extractor technique [186]						√								√
Elliptic Curve Diffie-Hellman (ECDH) [152]							√	√						
Key agreement									√	√	√			
Biohashing [187]						√								
Access polynomial [188]												√		
Elliptic curve cryptography [189]													√	√

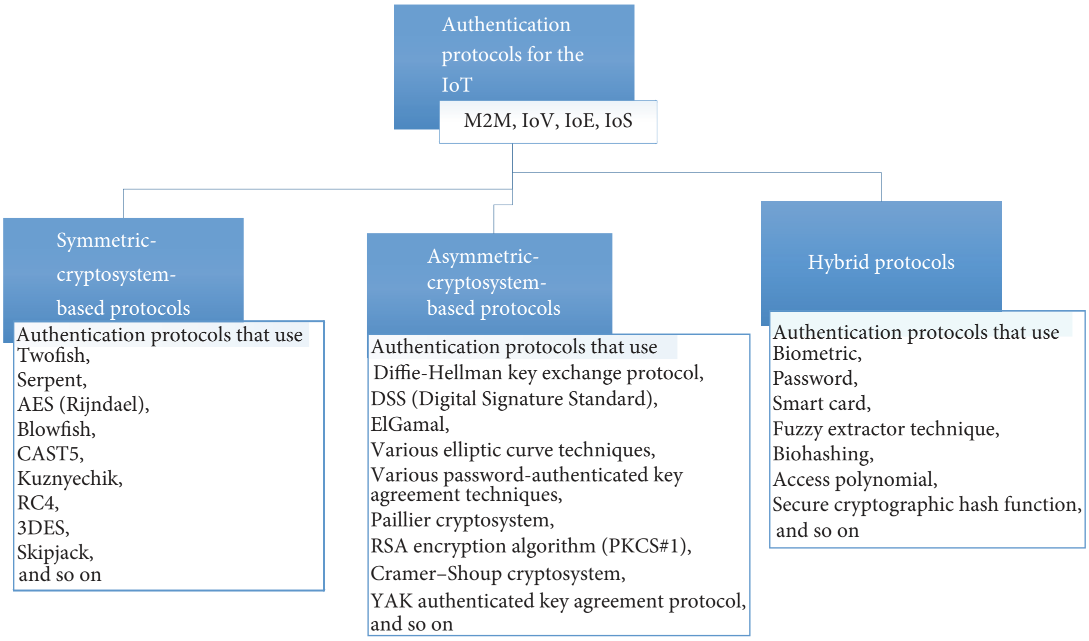

Authentication protocols for the IoT
M2M, IoV, IoE, IoS
Symmetric-cryptosystem-based protocols
Authentication protocols that use
Twofish,
Serpent,
AES (Rijndael),
Blowfish,
CAST5,
Kuznyechik,
RC4,
3DES,
Skipjack,
and so on
Asymmetric-cryptosystem-based protocols
Authentication protocols that use
Diffie-Hellman key exchange protocol,
DSS (Digital Signature Standard),
ElGamal,
Various elliptic curve techniques,
Various password-authenticated key agreement techniques,
Paillier cryptosystem,
RSA encryption algorithm (PKCS#1),
Cramer–Shoup cryptosystem,
YAK authenticated key agreement protocol,
and so on
Hybrid protocols
Authentication protocols that use
Biometric,
Password,
Smart card,
Fuzzy extractor technique,
Biohashing,
Access polynomial,
Secure cryptographic hash function,
and so on

Figure 9: Classification of the existing authentication protocols for the IoT based on the cryptosystems.

[184]. The Chebyshev Polynomial of degree p is defined by Mason and Handscomb [183] as $T_p(x) = \cos(pX \text{ acrcos } x)$ where the domain is the interval $x \in [-1, 1]$ with two properties [225]. However, three protocols, that is, [69–71], use the ID-based cryptography (IBC) [180]. On the other hand, the protocol [143] uses the Advanced Encryption Standard (AES) [185] such as the protocol [53]. The smart card-based authentication protocols are a very promising and practical solution to remote authentication [226], as presented in Table 15. There are five [72–75, 144] smart card-based authentication protocols where each protocol integrates a method with the smart card. For example, the protocol [72] uses the fuzzy extractor technique [186], where a fuzzy extractor is a pair of randomized procedures, "generate" (Gen) and "reproduce" (Rep), and is efficient if Gen and Rep run in expected polynomial time. For more details about the fuzzy extractor technique, we refer the reader to the paper [186]. In addition, the elliptic curve cryptography [189] is used by both protocols [77, 146].

4.2. Formal Security Verification Techniques. In order to prove the performance of an authentication protocol in terms of security, researchers use formal security verification techniques. As presented in Figure 10, there are five formal security verification techniques, namely, BAN-logic, analysis by process (Spi calculus), Game Theory, Automated

Table 15: The smart card-based authentication protocols.

Protocol	Type	Design goal
Das (2016) [72]	Remote authentication	Providing a user authentication to resolve the security weaknesses of the scheme [190]
Chang and Le (2016) [73]	Remote authentication	Providing mutual authentication and perfect forward secrecy
Jiang et al. (2016) [74]	Remote authentication	Providing mutual authentication, anonymity, and untraceability
Farash et al. (2016) [75]	Remote authentication	Providing the user authentication with traceability protection and sensor node anonymity
Srinivas et al. (2017) [144]	Remote authentication	Providing the mutual authentication with anonymity and unlinkability

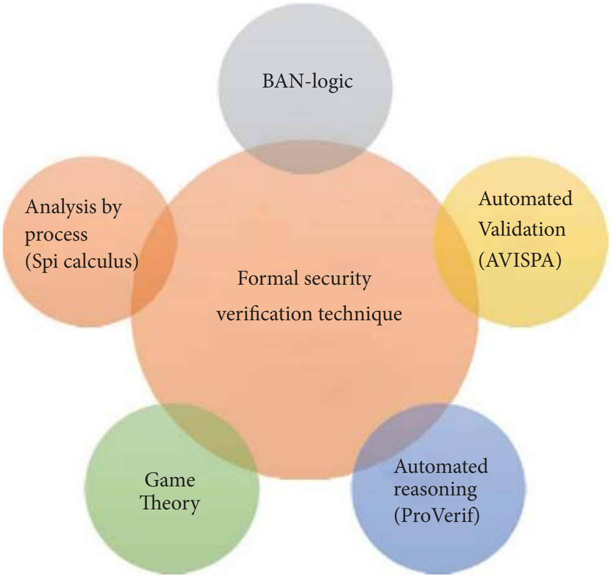

BAN-logic
Analysis by process (Spi calculus)
Automated Validation (AVISPA)
Formal security verification technique
Game Theory
Automated reasoning (ProVerif)

Figure 10: Formal security verification techniques used by the surveyed protocols.

reasoning (ProVerif), and Automated Validation (AVISPA). In addition, Table 16 presents the formal security verification techniques used in authentication protocols for the IoT.

The Burrows-Abadi-Needham Logic (BAN-logic) [195] is used by nine authentication protocols [68–70, 74–77, 144, 147]. A typical BAN-logic sequence includes three steps, (1) verification of message origin; (2) verification of message freshness; and (3) verification of the origin's trustworthiness. Therefore, the protocol [68] uses the BAN-logic to prove that the proposed protocol can establish a session key between user and sensor node. Both protocols [69, 77] use the BAN-logic in order to prove that the protocol has achieved mutual authentication and session key agreement securely. The protocol [144] uses the BAN-logic to prove that the protocol can resist numerous security attacks, which include the attacks, found in the Amin and Biswas's scheme [70]. There are seven authentication protocols [70, 72, 75, 142, 144, 147, 197] that use the Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]. The AVISPA tool provides a modular and expressive formal language for specifying security protocols and properties. The protocol [197] uses the AVISPA tool in order to prove that the proposed protocol is free from man-in-the-middle and replay attacks. The protocol [75] uses the AVISPA tool to prove that the protocol allows a user to establish a session key with a sensor node of his choice near the end of the authentication process. In addition, there are four authentication protocols [37, 38, 67, 146] that use the ProVerif tool [191], which is an automatic cryptographic protocol verifier, in the formal model, called Dolev-Yao model [196]. The protocol [38] uses the ProVerif tool in order to proof the mutual authentication between the mobile equipment and its serving network. The protocol [37] uses the ProVerif tool to prove that the proposed protocol can implement mutual authentication and key agreement between multiple devices and the core network simultaneously. The protocol [146] uses the ProVerif tool to prove that the proposed protocol can pass the verifications according to the Dolev-Yao model [196]. Finally, the protocol [73] uses a sequence of games under the decisional Diffie-Hellman (ECDDH) problem in order to proof that the protocol provides secure and perfect forward secrecy authentication. For more details about the game-theoretic approaches, we refer the reader to the survey [227].

5. Taxonomy and Comparison of Authentication Protocols for the IoT

In this section, we examine, in detail, authentication protocols developed for or applied in the context of IoT. As shown in Figure 11, the realization processes of an authentication protocol for IoT are based on the following processes:

(1) Definition of network model (e.g., M2M, IoV, IoE, and IoS).

(2) Definition of authentication model (e.g., mutual authentication, perfect forward secrecy, anonymity, and untraceability).

(3) Definition of attacks model (e.g., replay attack, stolen smart card attack, privileged-insider attack, offline password guessing attack, impersonation attack, and sensor node capture attack).

(4) Selection of countermeasures (e.g., cryptographic methods, Bloom Filter, biometric, Smart card, access polynomial, and Chebyshev Chaotic Maps).

(5) Proposition of main phases of the protocol (e.g., initial setup; registration process).

Table 16: Formal security verification techniques used in authentication protocols for the IoT.

Protocol	Approach	Main results
Lai et al. (2013) [38]	The security of the protocol is analyzed using the ProVerif tool [191]	Proof the mutual authentication between mobile equipment and its serving network

Shao et al. (2016) [63]	(i) Decisional Diffie-Hellman (DDH) Assumption;
	(ii) Decision Linear (DLIN) Assumption;
	(iii) Extended Computational Diffie-Hellman (eCDH) Assumption
	(iv) Computational Inverse Diffie-Hellman (ciCDH) Assumption
		(i) The proposed group signature scheme satisfies unforgeability
		(ii) The proposed group signature scheme satisfies anonymity
		(iii) The proposed theorem satisfies the traceability

Zhang et al. (2016) [65]	Based on the size of the beacon interval and the network bandwidth	Broadcasting the MAC of a message's prediction outcome is secure
Zhang et al. (2016) [52]	Bilinear Diffie-Hellman and the computational Diffie- Hellman assumptions	The protocol satisfies individual authentication, non-repudiation, vehicle privacy and traceability
Dolev et al. (2016) [66]	Spi calculus [192]	The proposed session key establishment protocol respects the authenticity property and the secrecy property
Chan and Zhou (2014) [48]	NXP-ATOP platform [193]	Demonstrate the two-factor cyber-physical device authentication
Lai et al. (2013) [37]	The security of the protocol is analyzed using the ProVerif tool [191]	The scheme can implement mutual authentication and key agreement between multiple devices and the core network simultaneously
Li and Cao (2011) [28]	Prove the existence of a pivot rank by contradiction	The total signing cost does not increase
Li et al. (2012) [138]	Diagnose tools	Detect failure points and to minimize the whole fault time
Nicanfar et al. (2014) [142]	Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	Providing mutual authentication and key management mechanisms
Mahmood et al. (2016) [67]	The security of the protocol is analyzed using the ProVerif tool [191]	Verifies mutual authentication and session key secrecy properties of the proposed scheme
Kumari et al. (2016) [68]	Burrows-Abadi-Needham Logic (BAN-logic) [195]	Prove that the proposed scheme establishes a session key between user and sensor node
Chung et al. (2016) [69]	Burrows-Abadi-Needham Logic (BAN-logic) [195]	Prove the validity of authentication and key agreement protocol
Amin and Biswas (2016) [70]	(i) Burrows-Abadi-Needham Logic (BAN-logic) [195]. (ii) Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	Prove that the protocol has achieved mutual authentication and session key agreement securely
Das (2016) [72]	Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	The scheme is secure against the replay and man-in-the-middle attacks against an adversary
Chang and Le (2016) [73]	Sequence of games under the decisional Diffie-Hellman (ECDDH) problem	The scheme provides secure and perfect forward secrecy authentication
Jiang et al. (2016) [74]	Burrows-Abadi-Needham Logic (BAN-logic) [195]	The improved scheme accomplishes mutual authentication and key agreement between the user and sensor, the user, and the gateway node
Farash et al. (2016) [75]	(i) Burrows-Abadi-Needham Logic (BAN-logic) [195] (ii) Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	Prove that the scheme allows a user to establish a session key with a sensor node of his choice near the end of the authentication process
Srinivas et al. (2017) [144]	(i) Burrows-Abadi-Needham Logic (BAN-logic) [195] (ii) Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	The scheme can resist numerous security attacks, which include the attacks, found in Amin and Biswas's scheme [70]

Table 16: Continued.

Protocol	Approach	Main results
Kumari et al. (2016) [76]	Burrows-Abadi-Needham Logic (BAN-logic) [195]	The scheme provides secure mutual authentication between a legal user and an accessed sensor node inside WSN or not
Jiang et al. (2017) [77]	Burrows-Abadi-Needham Logic (BAN-logic) [195]	Prove that an identity and a session key is agreed between the user and the sensor
Wu et al. (2016) [146]	The security of the protocol is analyzed using the ProVerif tool [191]	The scheme passes the verifications according to the Dolev-Yao model [196]
Das et al. (2016) [147]	(i) Burrows-Abadi-Needham Logic (BAN-logic) [195] (ii) Random oracle model (iii) Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	Prove secure mutual authentication between a legal user and an accessed sensor node
Das et al. (2016) [197]	Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [194]	The scheme is free from man-in-the-middle and replay attacks

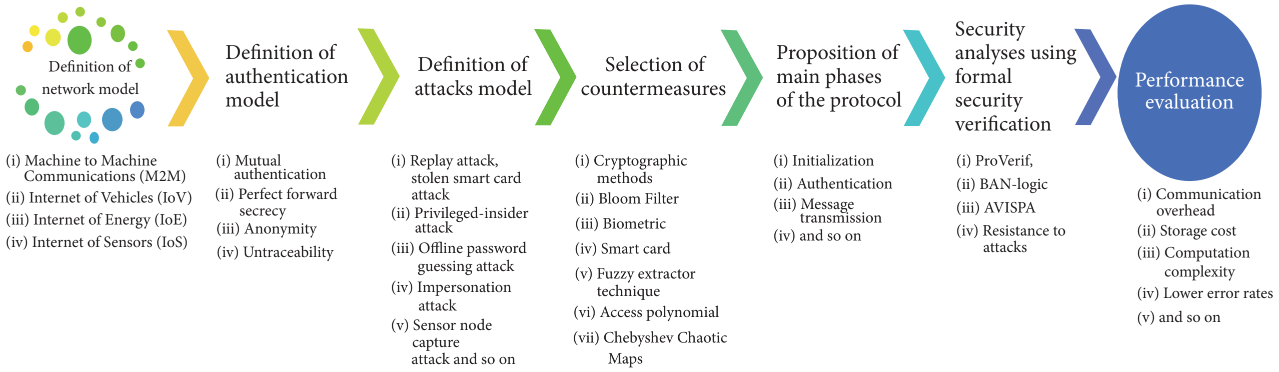

Definition of network model
Definition of authentication model
Definition of attacks model
Selection of countermeasures
Proposition of main phases of the protocol
Security analyses using formal security verification
Performance evaluation
(i) Machine to Machine Communications (M2M)
(ii) Internet of Vehicles (IoV)
(iii) Internet of Energy (IoE)
(iv) Internet of Sensors (IoS)
(i) Mutual authentication
(ii) Perfect forward secrecy
(iii) Anonymity
(iv) Untraceability
(i) Replay attack, stolen smart card attack
(ii) Privileged-insider attack
(iii) Offline password guessing attack
(iv) Impersonation attack
(v) Sensor node capture attack and so on
(i) Cryptographic methods
(ii) Bloom Filter
(iii) Biometric
(iv) Smart card
(v) Fuzzy extractor technique
(vi) Access polynomial
(vii) Chebyshev Chaotic Maps
(i) Initialization
(ii) Authentication
(iii) Message transmission
(iv) and so on
(i) ProVerif,
(ii) BAN-logic
(iii) AVISPA
(iv) Resistance to attacks
(i) Communication overhead
(ii) Storage cost
(iii) Computation complexity
(iv) Lower error rates
(v) and so on

Figure 11: The realization processes of an authentication protocol for the IoT.

(6) Security analyses using formal security verification (e.g., ProVerif, BAN-logic, and AVISPA).

(7) Performance evaluation (e.g., in terms of storage cost, computation complexity, communication overhead, and lower error rates).

Figure 12 presents the categorization of authentication models for the IoT. We note that some of the papers may be classified into multiple authentication models. We circumvented this ambiguity by classifying the papers according to the IoT environment, as presented in Figure 13, that is, (1) authentication protocols for M2M, (2) authentication protocols for IoV, (3) authentication protocols for IoE, and (4) authentication protocols for IoS.

5.1. Authentication Protocols for M2M. The surveyed papers of authentication protocols for Machine to Machine communications (M2M) as shown in Table 17 are published between 2012 and 2016. In order to speed up the process of authentication and avoid authentication signaling overload, Lai et al. [61] focused on the problem of group authentication and key agreement for resource-constrained M2M devices in 3GPP networks. Specifically, the authors proposed a novel group-based lightweight authentication scheme for resource constrained M2M, called GLARM. The network model used in [61] is based on 3GPP standard with three domains, including access networks, evolved packet core, and non-3GPP domain, for example, Internet. To guarantee the entity mutual authentication and secure key agreement, the GLARM scheme uses two main phases, namely, (1) Initialization phase and (2) Group authentication and key agreement phase. In addition, the GLARM scheme can ensure QoS for machine-type communications devices, but the computation complexity is much less than schemes [32, 38, 46]. In order to distinguish between different physical devices running the same software and detecting mimic attacks, Chen et al. [62] proposed an authentication protocol for the IoT, named S2M. The S2M protocol uses tree main phases, namely, (1) audio-handshake phase, (2) mixed-signal generation phase, and (3) feature extraction and storage phase. S2M can achieve variable distance authentication and active attack detection using acoustic hardware (Speaker/Microphone) fingerprints. In addition, S2M is efficient in terms of lower error rates compared with DISWN [198], LDTLS [199], PLTEA [200], and SeArray [201], but the performance of the methods in

Table 17: Summary of authentication protocols for M2M.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)
Lai et al. (2016) [61]	Based on 3GPP standard with three domains, including, access networks, evolved packet core, and non-3GPP domain, e.g., Internet	Guarantee the entity mutual authentication and secure key agreement	(i) Initialization phase (ii) Group authentication and key agreement phase	+ Resistance to DoS attack, redirection attack, and man-in-the-middle attack + Computation overheads are fairly small + Computation complexity is much less than schemes [32, 38, 46] + Can ensure QoS for machine-type communications devices − Some privacy models are not analyzed such as location privacy and identity privacy − Storage costs is not considered
Chen et al. (2017) [62]	Two wireless devices	Achieving variable distance authentication and active attack detection	(i) Audio-handshake phase; (ii) Mixed-signal generation phase (iii) Feature extraction and storage phase	+ Efficient in terms of lower error rates compared with DISWN [198], LDTLS [199], PLTEA [200], and SeArray [201] + Active attack detection (e.g., audio replay attack) − Privacy-preserving is not analyzed compared to the GLARM scheme [61] − Storage costs is not considered
Lai et al. (2014) [46]	3GPP-WiMAX-Machine-type Communication	Achieving mutual authentication and key agreement between all Machine-type Communication devices	(i) Initialization phase (ii) Roaming phase	+ Efficient in terms of the communication overhead compared to the traditional roaming authentication scheme and the optimized roaming authentication scheme in [34] + Efficient in terms of computation complexity compared to the scheme without aggregation − Resistance to attacks is not studied − Privacy-preserving is not analyzed compared to the GLARM scheme [61]. − Storage costs is not considered
Lai et al. (2013) [38]	3GPP standard with three domains, namely, access network domain, serving network domain and home network domain	Guarantee privacy-preservation and key forward/backward secrecy with	(i) Preparation and initialization (ii) Protocol execution for the first equipment (iii) Protocol execution for the remaining equipment of the same group (iv) Group member joining/leaving the group	+ Considers the data integrity and ensure user privacy + Resistance to attacks (DoS attack, redirection attack, man-in-the-middle attack, and replay attack) + The overhead of authentication message delivery of SE-AKA is lower than other existing AKA protocols + The computational overhead is larger than that of other traditional protocols such as the work [202] + Smaller storage costs than others protocols − Some privacy models are not analyzed such as location privacy and identity privacy

Table 17: Continued.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)
Fu et al. (2012) [34]	Mobile WiMAX networks with an access service network	Achieving mutual authentication and privacy preservation, and resisting the domino effect	(i) Predeployment phase (ii) Initial authentication phase (iii) Handover authentication phase	+ Efficient in terms of the computational and communication overhead compared to three schemes [39, 203, 204] + Considers the privacy preservation. − Storage costs is not considered − Resistance to attacks is not studied − No threat model presented − Error-detection and fault tolerance are not considered
Sun et al. (2015) [53]	Mobile users, home gateways, and an M2M server	Achieving a mutual authentication process in machine-to machine home network service	(i) Set-up (ii) Registration phase (iii) Login and authentication phase (iv) Update password phase (v) Home gateway joins the Time Division-Synchronous Code Division Multiple Access network	+ Efficient in terms of the amount of calculation and communication volume compared to the protocol in [205]. + Resistance to guessing attack, stolen-verifier attack, impersonation attack, and replay attack − Privacy-preserving is not analyzed compared to the GLARM scheme [61] − Storage costs is not considered − Lack nonrepudiation compared to the PBA scheme in [64]
Lai et al. (2014) [47]	Roaming network architecture with the home authentication center (HAC), the trust linking server (TLS), and the visiting authentication server (VAS)	(i) Providing a strong anonymous access authentication (ii) Guarantee user tracking on a disputed access request (iii) Achieving anonymous user linking and efficient user revocation for dynamic membership	(i) System initialization (ii) Roaming (iii) User tracking algorithm (iv) Anonymous user linking (v) User revocation	+ Efficient in terms of communication overhead and computation cost compared to two strong anonymous schemes [17, 26] + Considers the data integrity and ensure user privacy + Resistance to attacks, namely, Denial of Service (DoS) attack and impersonation attack − Some privacy models are not analyzed such as location privacy − Lack nonrepudiation compared to the PBA scheme in [64]
Zhu et al. (2015) [137]	Android smartphone devices	(i) Satisfy the user-friendliness with a reasonable false rejection rate (ii) Achieving an authentication process for Android smartphone devices	(i) Feature-set extraction and storing for registration (ii) Dual-factor authentication	+ Can enhance user-friendliness + Improve security without adding extra hardware devices − No threat model presented

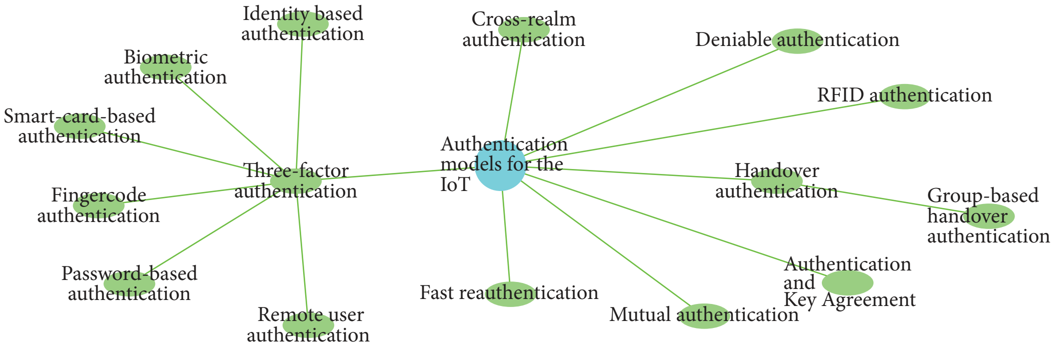

Identity based authentication
Cross-realm authentication
Deniable authentication
Biometric authentication
RFID authentication
Smart-card-based authentication
Authentication models for the IoT
Three-factor authentication
Handover authentication
Fingercode authentication
Group-based handover authentication
Authentication and Key Agreement
Password-based authentication
Fast reauthentication
Remote user authentication
Mutual authentication

Figure 12: Categorization of authentication models for the IoT.

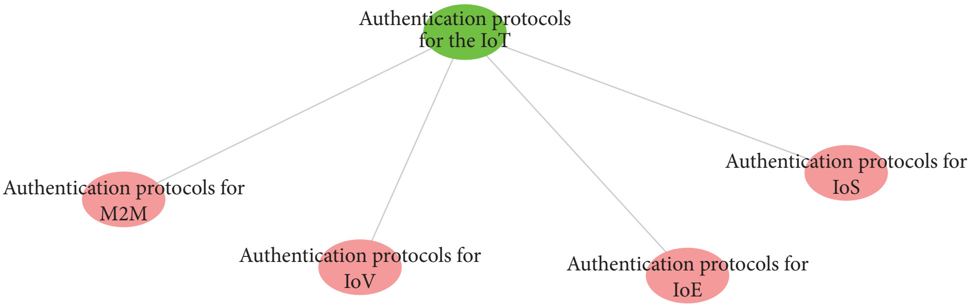

Authentication protocols for the IoT
Authentication protocols for IoS
Authentication protocols for M2M
Authentication protocols for IoV
Authentication protocols for IoE

Figure 13: Classification of authentication protocols for the IoT based on the IoT environment.

terms of privacy preservation is not analyzed, especially in comparison to the GLARM scheme [61].

To authenticate a group of devices at the same time, Lai et al. [46] proposed a scheme named SEGR. Based on roaming phase, SEGR can achieving mutual authentication and key agreement between all Machine-type Communication (MTC) devices when a group of MTC devices roams between 3GPP and WiMAX networks. SEGR is efficient in terms of the communication overhead computation complexity compared to the scheme in [34] and the scheme without aggregation, but again a comparison with other methods such as the GLARM scheme [61] regarding privacy preservation is missing. We also note that resistance to attacks of the SEGR method is not studied in the article as well [46]. To guarantee privacy preservation and key forward/backward secrecy, Lai et al. [38] proposed an efficient group authentication and key agreement protocol, called SE-AKA, which is based on authentication and key agreement (AKA) protocol. The overhead of authentication message delivery of SE-AKA is lower than other existing AKA protocols, but the computational overhead is larger than that of other traditional protocols such as the work [202]. In addition, SE-AKA has smaller storage costs than others AKA protocols. Similar to the SE-AKA protocol, Lai et al. in [37] proposed a lightweight group authentication protocol for M2M, called LGTH, which is efficient in terms of the signaling and computation overhead compared to the schemes [32, 228]. Similar to the SE-AKA & LGTH protocols, Fu et al. [34] proposed a group-based handover authentication scheme for mobile WiMAX networks. Based on the handover authentication phase, the work [34] is efficient in terms of the computational and communication overhead compared to three schemes [202–204], but the resistance to attacks is not studied and no threat model is presented.

In order to achieve a mutual authentication process in machine to machine home network service, Sun et al. [53] proposed an M2M application model for remote access to the intelligence home network service using the existing Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) system. The protocol [53] is efficient in terms of the amount of calculations needed and communication volume compared to the protocol in [205], but the article lacks a comparison of performance in terms of nonrepudiation against other schemes such as the PBA [64]. To achieve the authentication of mobile subscribers in the roaming service, Lai et al. [47] proposed a conditional privacy-preserving authentication with access linkability, called CPAL. The CPAL can (1) provide a strong anonymous access authentication, (2) guarantee user tracking on a disputed access request, and (3) achieve anonymous user linking and efficient user revocation for dynamic membership. The CPAL is efficient in terms of communication overhead and computation cost compared to two strong anonymous schemes [17, 26], but privacy aspects are not analyzed such as location privacy. Without adding any extra hardware devices, Zhu et al. [137] proposed a dual-factor authentication scheme, called Duth, designed for Android smartphone devices. Based on two main processes, namely, (1) feature-set extraction and storing for registration and (2) dual-factor authentication, the Duth scheme can satisfy the user-friendly requirements, along with a reasonable false rejection rate, providing on the same time an authentication process for Android smartphone devices.

Esfahani et al. [229] proposed a lightweight authentication scheme to ensure secure integration of Industrial Internet of Things (IIoT) solutions. Specifically, the work [229] considers an IIoT scenario where a machine equipped with a Secure Element (SE), is authenticated by a network element equipped with a Trusted Platform Module (TPM). Based on two procedures, namely, (a) the registration procedure and (b) the authentication procedure, the work [229] is characterized by low computational cost, communication, and storage overhead. However, based on the RF fingerprint of MTC devices' hardware, Zhao et al. [230] introduced the MTC architecture, as well as a cross-layer authentication scheme. The work [230] can facilitate the interoperation of heterogeneous MTC networks. In addition, Qiu and Ma [231] proposed an enhanced mutual authentication and key establishment scheme for the M2M communications in 6LoWPAN networks. Compared to the protocol [230], the work [231] is analyzed by the Protocol Composition Logic (PCL).

Amin et al. [232] proposed an architecture which is applicable for a distributed cloud environment using smart card. Using AVISPA tool and BAN-logic model, the protocol [232] is protected against user impersonation attack, replay attack, and session key discloser attack. Recently, Islam et al. [233] proposed a three-factor session initiation protocol (SIP) for multimedia big fata communications. Through the formal verification using the BAN-logic, the protocol is proved that can provide user anonymity and untraceability. To protect the confidential information in the device, Amin et al. [234] proposed a mutual authentication and key negotiation protocol. Based on the elliptic curve cryptography (ECC), the protocol [234] provides the mutual authentication property between the participants involved and provides a password update facility to registered users.

5.2. Authentication Protocols for IoV. The surveyed papers of authentication protocols for Internet of Vehicles (IoV) as shown in Table 18 are published between 2013 and 2016. Cespedes et al. in [39] considered the security association between asymmetric links during Vehicle to Vehicle (V2V) communications. More precisely, the authors proposed a multihop authenticated proxy mobile IP scheme, called MA-PMIP. Based on authentication phase and mobile router revocation, MA-PMIP can achieve less location update cost compared with the scheme [206] and the handover delay lower than the scheme [206]. In addition, MA-PMIP can achieve mutual authentication against authentication attacks but the privacy-preserving is not analyzed compared to the GLARM scheme [61]. In order to expedite message authentication in VANET, Wasef and Shen [40] proposed an expedite message authentication protocol, named EMAP. Based on the revocation checking process, EMAP can overcome the problem of the long delay incurred in checking the revocation status of a certificate using a certificate revocation list. EMAP is efficient in terms of computational complexity of revocation status checking and the authentication delay is constant and independent of the number of revoked certificates. Therefore, the question we ask here is can these protocols work well in the decentralized group model? The authentication scheme proposed recently by Shao et al. in [63] can answer this question where it can achieve two requirements for threshold authentication, namely, distinguishability and efficient traceability. The protocol in [63] is proven that is secured by three theorems; namely, (1) the proposed group signature scheme satisfies unforgeability, (2) the proposed group signature scheme satisfies anonymity, and (3) the proposed theorem satisfies the traceability.

To achieve the nonrepudiation in IoV, Lyu et al. in [64] proposed a lightweight authentication scheme called PBA. Based on the idea of Merkle hash tree construction and self-generated MAC storage, the PBA scheme can resist packet losses and maintain high packet processing rate with low storage overhead. The PBA is efficient in terms of overall delay compared to the TESLA scheme in [162] and the VAST scheme in [161]. Zhang et al. in [52] considers a VANET with four main entities, that is, key generator center (KGC), traffic management authority (TMA), RSUs, and vehicles. Based on identity-based aggregate signatures, the protocol in [52] can guarantee some properties such as message authentication, nonrepudiation, message confidentiality, privacy, and traceability. Similar to the scheme [52], Zhang et al. [65] proposed an efficient distributed aggregate privacy-preserving authentication protocol, called DAPPA, which is based on a new security tool called multiple-TA OTIBAS (MTA-OTIBAS). The DAPPA protocol can guarantee the conditional unlinkability, ideal tamper-proof device (TPD) freeness, and key escrow freeness. In addition, the DAPPA protocol is efficient compared to the ECDSA protocol in [163] and more efficient than the IBA scheme in [52] on average but lacks nonrepudiation compared to the PBA scheme in [64]. Based on monolithically certified public key and attributes, Dolev et al. [66] proposed an idea to ensure the countermeasures against the man-in-the-middle attack under the vehicle authentication. The work in [66] is efficient in terms of iteration cost compared to other existing Authenticated Key Exchange (AKE) protocols such as ISO-KE [207] and SIGMA [208]. To defend against coordinated cyber-physical attacks, Chan and Zhou [48] proposed a two-factor cyber-physical device authentication protocol, which can be applied in the IoV. Especially in the IoT, the vehicles may join or leave the platoon at any time in the platoon-based vehicular cyber-physical system. To guarantee anonymity of platoon members, Lai et al. [54] proposed a secure group setup and anonymous authentication scheme, named SGSA, for platoon-based vehicular cyber-physical systems. Based on the anonymous authentication with traceability phase, the SGSA scheme can provide strong anonymous access authentication.

Ferrag and Ahmim [235] proposed a recent scheme based on searchable encryption with vehicle proxy reencryption, called ESSPR, for achieving privacy preservation of message in the IoV environment. ESSPR is robust against eavesdropping attack, wormhole attack, packet analysis attack, packet tracing attack, and replay attack.

Table 18: Summary of authentication protocols for IoV.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)

Cespedes et al. (2013) [39]	A vehicular communications network with Access Routers (ARs) that connect the VANET to external IP networks	Achieving mutual authentication against authentication attacks	(i) Key establishment phase;
			(ii) MR registration phase;
			(iii) Authentication phase;
			(iv) Mobile router revocation
				+ Considers the asymmetric links in the VANET.
				+ Achieving less location update cost compared with the scheme [206].
				+ The handover delay lower than the one in the scheme [206].
				+ Resistance to replay attack, man-in-the-middle attack, and denial of service (DoS) attack.
				− Privacy-preserving is not analyzed compared to the GLARM scheme [61].
				− Lack nonrepudiation compared to the PBA scheme in [64]

Shao et al. (2016) [63]	VANET with some parties, including, central authority, tracing manager, many RSUs, and many OBUs	Guarantee unforgeability, anonymity, and traceability	Initialization stage;
			Registration stage;
			Join stage;
			Sign stage;
			Verify stage;
			Trace stage
				+ Efficient in terms of the computational cost of three operations, namely, Initialization, Registration, and Trace.
				+ Can prevent replay attacks.
				− No comparison with other schemes.
				− The communication overhead is not studied.
				− Lack nonrepudiation compared to the PBA scheme in [64]

Lyu et al. (2016) [64]	VANET with divide messages into two types (1) single-hop beacons and (2) multi-hop traffic data.	Guarantee some properties such as timely authentication, nonrepudiation, packet losses resistant, and DoS attacks resistant	(i) Chained keys generation;
			(ii) Position prediction;
			(iii) Merkle hash tree construction;
			(iv) Signature generation
				+ Considers the nonrepudiation.
				+ The computational cost reduces with the increasing of time frame.
				+ Can resist packet losses.
				+ Maintain high packet processing rate with low storage overhead.
				− Privacy-preserving is not analyzed compared to the GLARM scheme [61]

Zhang et al. (2016) [65]	Trusted authority (TA), a number of RSUs and vehicles	Guarantee the conditional unlinkability, ideal tamper-proof device (TPD) freeness, key escrow freeness	(i) Member secrets generation; (ii) Vehicle sign; (iii) Message verification and signature storage; (iv) Trace internal pseudo-identity (IPID) and authentication key update; (v) On-Line update	+ Efficient in terms of message authentication delay on average. + Considers privacy preserving. + Resistance to the side-channel attack, false messages attack, denial-of-service (DoS) attack, and Sybil attack. + Efficient compared to the ECDSA protocol in [163] and more efficient than the IBA scheme in [52] on average. − Lack nonrepudiation compared to the PBA scheme in [64]

Table 18: Continued.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)

Zhang et al. (2016) [52]	VANET with four main entities, i.e., key generator center (KGC), traffic management authority (TMA), RSUs and vehicles	Guarantee some properties such as message authentication, nonrepudiation, message confidentiality, privacy, and traceability	(i) System setup;
			(ii) Protocol for STP and STK distribution;
			(iii) Protocol for common string synchronization;
			(iv) Protocol for vehicular communications
				+ Efficient in terms of the average message delay and the verification delay.
				+ Efficient in terms of verification delay compared to the scheme in [166].
				+ Considers the nonrepudiation.
				+ Resistance to attacks, namely, message reply, message modification, movement tracking.
				− Location privacy is not considered

Dolev et al. (2016) [66]	The vehicle network is divided into the controller area network (CAN), local interconnect network (LIN), and media oriented system (MOST)	Ensure the countermeasures against the Man-in-the-Middle attack under the vehicle authentication	(i) System settings;
			(ii) Certificate authority;
			(iii) Vehicular attributes
				+ Efficient in terms of iteration cost compared to the existing Authenticated Key Exchange (AKE) protocols such as ISO-KE [207] and SIGMA [208].
				+ Resistance to attacks, namely, Man-in-the-Middle attack and impersonation attack.
				− Privacy-preserving is not analyzed compared to the GLARM scheme [61]

Chan and Zhou (2014) [48]	Smart grid electric vehicle ecosystem	Provides assurance of the digital identity and the device's controllability in the physical domain	(i) Communication settings; (ii) Cyber-physical device authentication	+ Resistance to substitution attacks. − No comparison with other schemes. − The average message delay and the verification delay are not evaluated

5.3. Authentication Protocols for IoE. The surveyed papers of authentication protocols for Internet of Energy (IoE) as shown in Table 19 are published between 2011 and 2016. We noted here that we have reviewed some authentication protocols proposed for secure smart grid communications in our survey in [219], namely, the schemes in [236]. In this subsection, we will review only the works that are not reviewed in the survey [219].

To provide multicast authentication in smart grid, Li and Cao [28] proposed the scheme Tunable Signing and Verification (TSV). Specifically, TSV combines Heavy signing light verification (HSLV) and Light Signing Heavy Verification (LSHV) to achieve a flexible tradeoff between the two. TSV can reduce the storage cost, but the privacy-preserving is not discussed and the reports' confidentiality and integrity are not considered compared to the scheme [49]. The smart meters are planning to reduce the time intervals to 1 min or even less. For this, Li et al. [49] developed a Merkle-tree-based authentication scheme to minimize computation overhead on the smart meters. The work [49] is efficient in terms of computation complexity of the HAN user and the neighborhood gateway compared to the Rivest–Shamir–Adleman (RSA)-based authentication scheme [237]. Therefore, Li et al. [138] fixed the single-point failure in smart grid by proposing the idea of deploying a fault tolerance architecture to execute the authentication approach without any additional configuration or setup. Based on both main processes, namely, (1) batch verification and trinary diagnose TreeBatch and (2) signature amortization for Package Blocks, the work [138] can legalize the data aggregation with tremendously less signing and verification operations.

Nicanfar et al. [139] addressed the key management for unicast and multicast communications in the smart grid. The work [154] proposed a scheme for the mutual authentication between the smart grid utility network and Home Area Network smart meters, called SGAS-I, which can increase performance of the key management and does not cause any security drawback. Based on the multicast key support phase, SGAS-I can provide simplicity and low overhead, but the reports' confidentiality and integrity are considered

Table 19: Summary of authentication protocols for IoE.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)

Li and Cao (2011) [28]	Smart Grid with wide multicast applications, namely, wide area protection, demand-response, operation and control, and in-substation protection	Provide multicast authentication	(i) Key generation;
			(ii) Signing;
			(iii) Verification
				+ Efficient in terms of hash or one-way function invocations compared to the scheme [209].
				+ Resistance to message forgery attacks.
				+ Can reduce the storage cost.
				− Privacy-preserving is not discussed.
				− The reports' confidentiality and integrity are not considered compared to the scheme [49]

Li et al. (2014) [49]	Communication between the home area networks (HANs) and the neighborhood gateway using WiFi technology	(i) Detecting the replay attacks;
		(ii) Providing authentication for the source of electricity consumption reports;
		(iii) Guarantees the reports' confidentiality and integrity
			(i) System initialization;
			(ii) Report generation;
			(iii) Neighborhood gateway authentication
				+ Efficient in terms of computation complexity of the HAN user and the neighborhood gateway compared to the RSA-based authentication scheme.
				+ Efficient in terms of communication overhead between the HAN user and the neighborhood gateway compared to the RSA-based authentication scheme.
				+ Resistance to attacks, namely, replay attack, message injection attack, message analysis attack, and message modification attack.
				+ Guarantees the reports' confidentiality and integrity compared to the scheme [28].
				− The routing attacks are not considered such as wormhole attack

Li et al. (2012) [138]	The smart grid with power generation, power transmission, and power distribution	Providing the authentication for power usage data aggregation in Neighborhood Area Network (NAN) with fault tolerance architecture.	(i) Key generation;
			(ii) Signature generation;
			(iii) Batch verification and trinary diagnose TreeBatch;
			(iv) Signature amortization for Package Blocks
				+ Makes significant performance gains in terms of the communication and computation cost.
				+ Considers the fault diagnosis.
				− No threat model presented

Nicanfar et al. (2011) [139]	(i) The data communication in outside of the Home Area Network (HAN). (ii) Some smart meters and a utility server under a wireless mesh network topology	Providing mutual authentication scheme to prevent brute-force attacks, replay attacks, Man-In-The-Middle (MITM) attack, and Denial-of-Service (DoS) attacks	(i) Initialization; (ii) Ongoing maintenance or Short period key refreshment; (iii) Long period key refreshment; (iv) Multicast key support	+ Can provide simplicity and low overhead. + Resistance to attacks, namely, brute-force attacks, replay attacks, Man-In-The-Middle (MITM) attack, and Denial-of-Service (DoS) attacks. + Can provide secure key management. − The reports' confidentiality and integrity are considered compared to the scheme [49]

Chim et al. (2011) [140]	Smart grid network with three basic layers, namely, power generators, substations, and smart meters and smart appliances	Guarantee the message authentication, identity privacy, and traceability	(i) Preparation module;
			(ii) Pseudo-identity generation module;
			(iii) Signing module;
			(iv) Verification module;
			(v) Tracing module
				+ Requires only an additional 368 msec for HMAC signature verification at a substation.
				+ Efficient in overall normal traffic success rate when under attack.
				+ The message overhead is only 20 bytes per request message.
				− The routing attacks are not considered such as wormhole attack.
				− Storage costs are not considered.
				− No comparison with other schemes

Fouda et al. (2011) [141]	Smart grid with the power Distribution Network (DN), the Transmission Substation (TS), and a number of Distribution Substations (DSs)	Providing mutual authentication and achieving message authentication in a light-weight way	(i) Key generation;
			(ii) Message generation;
			(iii) Hash-based message authentication
				+ Efficient in terms of communication overhead and message decryption/verification delay compared to ECDSA-256.
				+ Resistance to attacks, namely, replay attack, chosen-plaintext attack, and collision attack.
				− Location privacy is not considered.
				− Identity privacy and traceability are not considered compared to the scheme [140]

Table 19: Continued.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)
Nicanfar et al. (2014) [142]	Multigate communication network proposed in [210]	Providing mutual authentication and key management mechanisms	(i) SGMA scheme (System setup; Mutual authentication Scheme) (ii) SGKM protocol (Key refreshment; Multicast key mechanism; Broadcast key mechanism)	+ Can prevent the adversary from continuing the successful attack. + Can prevent various attacks while reducing the management overhead. − Storage costs are not considered. − Lack nonrepudiation compared to the PBA scheme in [64]
Chim et al. (2015) [55]	Smart grid network based on hierarchical architecture, i.e., HANs, BANs, NANs	Providing the privacy-preserving recording and gateway-assisted authentication	(i) Preparation phase; (ii) Power plan submission phase; (iii) Power plan processing phase; (iv) Reconciliation phase; (v) System master secret updating phase	+ The message filtering at gateway smart meters can be helpful in reducing the impact of attacking traffic. + The privacy preserving and traceability are considered. − No comparison with other schemes. − Distributed denial of service (DDoS) attacks is not considered

Mahmood et al. (2016) [67]	The system model is homogeneous to the model in [49]	Detect and omit some attacks, namely, replay, false message injection, message analysis and modification attacks	(i) Initialization;
			(ii) Authentication;
			(iii) Message transmission
				+ Efficient in terms of communication cost and computation cost compared to the schemes [30, 35].
				+ Resistance to attacks, namely, replay, false message injection, message analysis and modification attacks.
				+ The reports' confidentiality and integrity are considered.
				− Location privacy is not considered

compared to the scheme [49]. To guarantee the message authentication with identity privacy and traceability, Chim et al. [140] proposed a scheme, called PASS, for the hierarchical structure of a smart grid. The PASS scheme focuses only on the substation-to-consumer subsystem where the real identity of any smart appliance can only be known by the control center using the concept of pseudo identity. Similar to the PASS scheme, Fouda et al. [141] proposed a scheme that can only provide an authenticated and encrypted channel for the late successive transmission but can also establish a semantic-secure shared key in the mutual authentication environment. The work in [141] is efficient in terms of communication overhead and message decryption/verification delay compared to ECDSA-256, but the identity privacy and traceability are not considered compared to the scheme [140].

In order to provide the mutual authentication between smart meters and the security and authentication server in the smart grid using passwords, Nicanfar et al. [142] proposed a mutual authentication scheme and a key management protocol, called SGMA and SGKM, respectively. The SGMA scheme concentrates on data communications over the advanced metering infrastructure (AMI) outside of the HAN domain, where each node has a unique ID and each smart meter has a unique serial number SN embedded by the manufacturer and an initial secret password. On the other hand, the SGKM protocol concentrates on node-to-node secure communications, where the nodes have the appropriate private–public keys to be used for unicast. Based on the multicast key mechanism, the SGMA scheme can prevent various attacks while reducing the management overhead but lack nonrepudiation compared to the PBA scheme in [64]. Shim et al. [55] consider a smart grid network based on hierarchical architecture, that is, HANs, BANs, and NANs. The work [55] proposed privacy-preserving recording and gateway-assisted authentication of power usage information. The message filtering at gateway smart meters can be helpful in reducing the impact of attacking traffic. Similar to the scheme [55], Mahmood et al. [67] proposed a lightweight message authentication scheme. Based on two main processes, namely, (1) authentication and (2) message transmission, the scheme [67] can detect and omit some attacks, namely, replay, false message injection, message analysis, and modification attacks. In addition, the scheme [67] is efficient in terms of communication cost and computation cost compared to the schemes [30, 35], but the location privacy is not considered.

5.4. Authentication Protocols for IoS. The surveyed papers of authentication protocols for Internet of Sensors (IoS) as shown in Table 20 are published in 2016. We noted here that we have reviewed some authentication protocols proposed for ad hoc social network (an application of WSN) in our survey in [220]. In this subsection, we will review only the works that are not reviewed in the survey [220] and the articles published in 2016 related to authentication protocols for IoS. For more details about the articles published before 2016, we refer the reader to six surveys published in 2013, 2014, and 2015, namely, [238–243].

Table 20: Summary of authentication protocols for IoS (Published in 2016).

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)

Kumari et al. (2016) [68]	Wireless sensor network (WSN) with the service seeker users, sensing component sensor nodes (SNs) and the service provider base-station or gateway node (GWN)	Providing mutual authentication with forward secrecy and wrong identifier detection mechanism at the time of login	(i) Initialization phase;
			(ii) User registration phase;
			(iii) Login phase;
			(iv) Authentication & key agreement phase;
			(v) Password change phase
				+ The user is anonymous.
				+ Resistance to attacks, namely, user impersonation attack, password guessing attack, replay attack, stolen verifier attack, smart card loss attack, session-specific temporary information attack, GWN Bypass attack, and privileged insider attack.
				+ Provides a secure session-key agreement and forward secrecy.
				+ Provides freely password changing facility.
				+ Efficient in unauthorized login detection with wrong identity and password.
				− The data integrity is not considered

Chung et al. (2016) [69]	Wireless sensor networks for roaming service	Providing an enhanced lightweight anonymous authentication to resolve the security weaknesses of the scheme [60]	(i) Registration phase; (ii) Login and authentication phase; (iii) Password change phase	+ Considers anonymity, hop-by-hop authentication, and untraceability. + Resistance to attacks, namely, password guessing attack, impersonation attack, forgery attack, known session key attack, and fair key agreement. − Location privacy is not considered

Gope and Hwang (2016) [71]	Real-time data access in WSNs	Ensuring the user anonymity, perfect forward secrecy, and resiliency of stolen smart card attacks	(i) Registration phase;
			(ii) Anonymous authentication and key exchange phase;
			(iii) Password renewal phase;
			(iv) Dynamic node addition phase
				+ Considers the user anonymity and untraceability.
				+ Provides perfect forward secrecy.
				+ Security assurance in case of lost smart card.
				+ Resilience against node capture attack and key compromise impersonation Attack.
				− The average message delay and the verification delay are not evaluated

Chang and Le (2016) [73]	Users, sensor nodes, and gateway node in WSN	Providing mutual authentication and perfect forward secrecy	(i) Registration phase;
			(ii) Authentication phase;
			(iii) Password changing phase
				+ Considers the session key security, perfect forward secrecy, and user anonymity.
				+ Resistance to attacks, namely, replay attack and smart card lost attack.
				+ Efficient in terms of computation cost in the authentication phases compared to the schemes [42, 50, 51, 211].
				− Privacy-preserving is not analyzed compared to the GLARM scheme [61].

Jiang et al. (2016) [74]	Users, sensor nodes, and gateway node in WSN.	Providing mutual authentication, anonymity, and untraceability	(i) Registration phase; (ii) Login and authentication phase	+ Provides mutual authentication, session key agreement, user anonymity, and user untraceability. + Resistance to attacks, namely, smart card attack, impersonation attack, modification attack, man-in-the-middle attack, and tracking attack. − Wormhole attack and blackhole attack are not considered

Table 20: Continued.

Prot.	Network model	Goals	Main processes	Performances (+) and limitations (−)

Farash et al. (2016) [75]	Users, sensor nodes, and gateway node in WSN	Providing the user authentication with traceability protection and sensor node anonymity	(i) Predeployment phase;
			(ii) Registration phase;
			(iii) Login and authentication phase;
			(iv) Password change phase
				+ Efficient in terms of communication, computation and storage cost compared to the scheme [51]
				+ Resistance to attacks, namely, replay attack, privileged-insider attack, man-in-the-middle attack, insider and stolen verifier attack, smart card attack, impersonation attack, bypassing attack, many logged-in users with the same login-id attack, password change attack, and DoS attack.
				− Wormhole attack and blackhole attack are not considered

Kumari et al. (2016) [76]	Users, sensor nodes, and gateway node in WSN	Providing the mutual authentication with traceability and anonymity	(i) Offline sensor node registration phase;
			(ii) User registration phase;
			(iii) Login phase;
			(iv) Authentication and key agreement phase;
			(v) Password update phase;
			(vi) Dynamic sensor node addition phase
				+ Efficient in terms of end-to-end delay (EED) (in seconds) and throughput (in bps).
				+ Efficient in terms of computation cost in login and authentication phases compared to both schemes Turkanović et al. [51] and Farash et al. [75].
				+ Resistance to attacks, namely, replay attack, stolen smart card attack, privileged-insider attack, offline password guessing attack, impersonation attack, and sensor node capture attack.
				− Wormhole attack and blackhole attack are not considered.
				− Lack nonrepudiation compared to the PBA scheme in [64].

Sun et al. (2016) [145]	Multicast communications in WSNs, including, sink and many groups, and each group has a powerful node and many low ordinary nodes	Providing the broadcast authentication and enhanced collusion resistance	(i) Initialization;
			(ii) Broadcast;
			(iii) Group keys' recovery and pairwise keys' updating;
			(iv) Node addition;
			(v) Node revocation
				+ Collusion resistance
				+ Resistance to attacks, namely, PKE-attack and PF-attack.
				− The end-to-end delay and throughput are not evaluated compared to the scheme [76].
				− Replay attack is not considered

Jiang et al. (2017) [77]	Users, sensor nodes, and gateway node in WSN	Achieving mutual authentication among the communicating agents with user anonymity and untraceability	(i) Registration phase;
			(ii) Login phase;
			(iii) Authentication phase;
			(iv) Password change phase
				+ Resistance to attacks, stolen-verifier attack, guessing attack, impersonation attack, modification attack, man-in-the-middle attack, and replay attack.
				− The end-to-end delay and throughput are not evaluated compared to the scheme [76].
				− Collusion resistance is not considered compared to the scheme [145]

Kumari et al. [68] reviewed and examined both schemes proposed by Li et al. in [42] and He et al. in [57] for its suitability to WSNs. Based on the results of this analysis, the authors proposed a chaotic maps based user-friendly authentication scheme for WSN with forward secrecy and wrong identifier detection mechanism at the time of login. The idea is to establish a session key between user and sensor node (SN) using extended chaotic maps. The scheme of Kumari et al. [68] is efficient in unauthorized login detection with wrong identity and password, but the data integrity is not considered. Similar to [68], Chung et al. [69] reviewed and examined the scheme [60]. Based on the security weaknesses of the scheme [60], the work [69] proposed an enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in WSN. Using three phases, namely, (1) registration phase, (2) login and authentication phase, and (3) password change phase, the work [69] can provide anonymity, hop-by-hop authentication, and untraceability, but location privacy is not considered.

Jan et al. [143] proposed an extremely lightweight payload-based mutual authentication, called PAWN, for the cluster-based hierarchical WSN. The PAWN scheme is based on two main phases, namely, (1) token-based cluster head election and (2) payload-based mutual authentication. With phase 1, the higher-energy nodes perform various administrative tasks such as route discovery, route maintenance, and neighborhood discovery. The authentication procedure is accomplished using the cooperative neighbor × neighbor (CNN) [244], that is, session initiation, server challenge, client response and challenge, and server response. The PAWN scheme is efficient in terms of average energy consumption and Handshake duration compared to the LEACH-C scheme in [245] and the SecLEACH scheme [246], but the privacy preservation is not analyzed compared to other methods, such as the GLARM scheme [61]. Based on the security weaknesses of the scheme [51], Amin and Biswas [70] proposed a secure lightweight scheme for user authentication and key agreement in multigateway based WSN. The scheme [70] is efficient in terms of computational cost, storage, and communication cost compared to the schemes [31, 36, 41, 45, 51]. In addition, the scheme [70] can provide much less energy consumption of the sensor nodes and user anonymity.

For the security of real-time data access in WSNs, Gope and Hwang [71] proposed an authentication protocol to ensure the user anonymity, perfect forward secrecy, and resiliency of stolen smart card attacks. The protocol [71] is efficient in terms of computational and communication cost compared to the schemes [31, 41, 72, 190, 247]. Based on the security weaknesses of the scheme [190], Das [72] proposed a secure and robust temporal credential-based three-factor user authentication scheme. The scheme [72] uses a biometric password and smart card of a legal user. The simulation results of the scheme [72] demonstrate that it is efficient in terms of computational and communication overhead compared to the schemes [41, 248, 249]. Based on the weaknesses in Turkanović et al.'s protocol [51], Chang and Le [73] proposed a flexible authentication protocol using the smart card for WSNs, which operates in two modes, namely, (1) providing a lightweight authentication scheme and (2) an advanced protocol based on ECC, which provides perfect forward secrecy. Both these two modes are efficient in terms of computation cost in the authentication phases compared to the schemes [42, 50, 51, 211].

Trying to deal with the weaknesses of the scheme presented in [57], Jiang et al. [74] proposed an untraceable two-factor authentication scheme based on elliptic curve cryptography. The scheme [74] is efficient in terms of computational cost compared to previous schemes [31, 50, 57, 211, 250], but the performance of the system under common attacks such as the wormhole attack and the blackhole attack is not presented. Based on the weaknesses in the scheme [51], Farash et al. [75] proposed an efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. The scheme [75] is efficient in terms of communication, computation, and storage cost compared to the scheme [51], but again the performance of the system under the wormhole attack or the blackhole attack is not presented. Based on the weaknesses in Amin and Biswas's scheme [70], Srinivas et al. [144] proposed a user authentication scheme for multigateway WSNs. The scheme [144] is efficient in terms of communication overhead during the login and authentication phase compared to the schemes [21, 70], but the performance of the system in terms of privacy preservation is not analyzed compared to previous methods, such as the GLARM scheme [61]. Similar to both schemes [74, 144], Kumari et al. [76] pointed out that the scheme of Farash et al. [75] is insecure against some attacks. The work presented in [76] especially is efficient not only in terms of end-to-end delay (EED) (in seconds) and throughput (in bps), but also in terms of computation cost in login and authentication phases compared to both schemes by Turkanović et al. [51] and Farash et al. [75].

Sun et al. [145] considered the multicast communications in WSNs, including, sink and many groups, where each group may have a powerful node and many low ordinary nodes. The powerful node acts as the group manager (GM) and is responsible for network security management, such as key issues, updating, revocation, and intrusion detection. Then, the authors reviewed and examined the scheme [188] in order to propose a scheme that considers the forward security, backward security, and collusion resistance. Based on the idea of access polynomial, the Sun et al. scheme [145] is efficient in terms of storage, computation, and communication overhead, but the replay attack is not considered. Jiang et al. proposed a scheme [77] that can achieve mutual authentication among the communicating agents with user anonymity and untraceability. In addition, the Jiang et al. scheme [77] is efficient in terms of computational cost compared to the schemes in [31, 50, 211, 250], but the collusion resistance is not considered compared to the scheme in [145].

Based on the weaknesses in the scheme [251], Wu et al. [146] proposed an improved three-factor authentication scheme for WSNs, which can be resistant to the desynchronization attack. Das et al. [147] reviewed the recently proposed Chang–Le's two protocols [73] and then showed that their protocols are insecure against some known attacks. Liu and Chung [148] proposed a secure user authentication scheme for wireless healthcare sensor networks, which is efficient in terms of computation cost compared to both schemes in [252, 253]. Gope et al. [254] proposed a special idea for resilience of DoS attacks in designing anonymous user authentication protocol. Combining three techniques, namely, smart card, password, and personal biometrics, Das et al. [197] proposed a three-factor user authentication and key agreement scheme based on multigateway WSN architecture. The scheme [197] is efficient in terms of computational, communication, and energy costs. Benzaid et al. [255] proposed an accelerated verification of digital signatures generated by BNN-IBS [256], which is an idea inspired by the acceleration technique of Fan and Gong [257].

6. Open Issues

6.1. M2M Open Issues. M2M communications can facilitate many applications, like e-health, smart grids, industrial automation, and environmental monitoring but on the same time face various security threats and trust issues. In e-health especially authentication of the devices must be robust to attacks that could threaten the correct exchange of information and consequently the life of the patient. In order to safely share and manage access to information in the healthcare system, it is essential to be able to authenticate users, including organizations and people. In Australia authentication is achieved through the use of digital certificates that conform to the Australian Government endorsed Public Key Infrastructure (PKI) standard, through the National Authentication Service for Health (NASH), but thorough research of the resistance to attacks of this and other similar systems is needed in order to reassure its robustness. Scalability and Heterogeneity are a rather general problem when dealing with M2M communication of devices that come from different vendors and using different operating systems. Solutions that focus only to Android devices [137] cannot guarantee end-to-end security of the system.

6.2. IoV Open Issues. Although a number of authentication protocols have been proposed recently which are capable of guaranteeing authentication for a network of vehicles, there are still open issues that need to be addressed by the research community.

6.2.1. Autonomous Driving. Until now anonymity of platoon members has been addressed in [54], which is capable of providing strong anonymous access authentication to the members of the platoon. Taking one step further and dealing with full automated vehicles that will be able to create platoons on the fly, with no central entity or trust authority in reach, novel authentication methods where vehicles can run by themselves must be developed. This could be done using several techniques. One method would be to use digital signatures, where each vehicle holds its own signing key and can verify its identity by signing challenges, combined with a defense mechanism that can face MITM attacks. Other methods could be the use of the trust levels of every vehicle using methods similar to [258].

6.2.2. Heterogeneous Vehicular Networking. The design, development, and deployment of vehicular networks are boosted by recent advances in wireless vehicular communication techniques, such as dedicated short-range communications (DSRC), Long-Term Evolution (LTE), IEEE 802.11p, and Worldwide Interoperability for Microwave Access (WiMax). Novel protocols that can be deployed on all these communication channels and can guarantee authentication under attacks that can be initiated from each one of these networks are an area of future research. Safeguarding one communication channel without dealing with the threats that all these networks face will leave the IoV vulnerable to several kinds of attacks against authentication.

6.2.3. Social Internet of Vehicles. Social Internet of Vehicles (SIoV) describes the social interactions both among vehicles [259] and among drivers [260]. Ensuring authentication in the communication among vehicles cannot guarantee full protection of identities of entities if the social notion of communication is neglected [125]. Future authentication-enhancing technologies for SIoVs should be based on proven authentication-enhancing technologies for social networks and vehicular networks.

6.3. IoE Open Issues. Based on the definition of the Internet of Energy as an integrated dynamic network infrastructure based on standard and interoperable communication protocols that interconnect the energy network with the Internet allowing units of energy to be dispatched when and where it is needed, it is easily understood that authentication in the IoE environment is not an easy problem to solve. IoE combines M2M, V2G, IIoT (industrial Internet of things), Smart home automation, cloud services, and IoS. It would be better to define IoE as an application of the IoT on the Energy domain. Authentication on the IoE domain cannot be reassured without dealing with each of the aforementioned subdomains. Security [261] and hardware [262] authentication techniques along with solutions dealing with middleware security [263] must be combined.

6.4. IoS Open Issues. The major problems that the IoS networks have to face are energy efficiency and security assurance of the sensors. Intrusion Detection Systems (IDSs) and energy efficient mechanisms are not thoroughly investigated and resolved in the surveyed authentication protocols for the IoS. Raza et al. [264] proposed an idea based on real-time intrusion detection for the IoT, called SVELTE. Mechanisms that can extend the SVELTE scheme for the IoS in order to be energy efficient would be a possible research direction. Hence, future works addressing both security, mainly IDSs, and energy will have an important contribution for the authentication protocols. In addition, we believe further research is needed to develop a new framework for combining intrusion detection systems and authentication protocols for detecting and avoiding attacks in IoS.

6.5. Pattern Recognition and Biometrics for the IoT. Hybrid authentication protocols are based on two methods for identifying an individual, including, knowledge-based (e.g., the passwords) and token-based (e.g., the badges). Each method has its weakness; that is, (1) the password can be forgotten or guessed by an adversary and (2) the badge can be lost or stolen. Nevertheless, the safest way is the use of biometric characteristics because two people cannot possess exactly the same biometric characteristic. Hence, future works addressing pattern recognition authentication techniques along with biometrics will have an important contribution in improving authentication in the IoT. Recently new promising efforts that apply biometrics on IoT have been proposed [265] and the term of Internet of biometric things

(IoBT) has been introduced [266]. Biometric technology on the other hand raises privacy and ethical issues that need to be taken in mind when designing new authentication protocols, especially for applications that deal with critical data [267].

6.6. Authentication for the IoT Applications in 5G. The development of 5G networks is driven by IoT connectivity, where the IoT applications have been categorized into two classes: massive machine-type communications (mMTC) and ultrareliable low-latency communications (URLLC), as discussed by Schulz et al. [268]. As mobile devices will be connected to the network all the time, the IoT applications can more easily be tracked down and are more vulnerable to several types of attacks, like impersonation, eavesdropping, man-in-the middle, denial of service, replay, and repudiation attack [269]. One possible future direction is to develop an authentication protocol for the IoT applications in 5G.

6.7. Lessons Learned. From the threat models in M2M, IoV, IoE, and IoS, we found thirty-five attacks discussed by the surveyed protocols. Therefore, we were able to classify the formal security verification techniques into five techniques, namely, BAN-logic, analysis by process, Game Theory, Automated reasoning (ProVerif), and Automated Validation (AVISPA). In addition, based on the cryptosystems, we were able to classify the authentication protocols for the IoT into three categories, namely, symmetric-cryptosystem based protocols, asymmetric-cryptosystem-based protocols, and hybrid protocols.

After conducting a comprehensive survey of authentication protocols, we see that the reliability of an authentication protocol depends not only on the effectiveness of the cryptography method used against attacks but also on the computation complexity and communication overhead. Therefore, in order to guarantee authentication between the machines for the IoT, we invite well-positioned researchers and practitioners to propose authentication frameworks that cover not only one but three layers, namely, the application layer, the network layer, and the sensing layer. In this paper, we also see a need for a comprehensive survey for privacy-preserving schemes for the IoT under four environments, including, M2M, IoV, IoE, and IoS.

Authentication protocols for the IoT may be improved in terms of (1) addressing both the authentication and privacy problem, (2) developing efficient IDSs, (3) improving the computation complexity of the proposed methods, (4) improving the communication overhead of the methods, (5) developing of formal security verification techniques, (6) accounting of the process of detecting and avoiding attacks, and (7) capturing of experts opinion in the field of computer security.

7. Conclusion

In this paper a structured comprehensive overview of authentication protocols for the IoT is presented. These protocols can be categorized based on the target environment, for example, Machine to Machine Communications (M2M), Internet of Vehicles (IoV), Internet of Energy (IoE), and Internet of Sensors (IoS). Major threats, countermeasures, and formal security verification techniques used by state-of-the-art authentication protocols are presented. A side-by-side comparison in a tabular form for the current state-of-the-art of authentication protocols proposed for M2M, IoV, IoE, and IoS is also provided. Based on this analysis future research directions are given. Authentication protocols for the IoT may be improved in terms of being able to cover both authentication and privacy and be more efficient in terms of computation complexity and communication overhead as long as they are able to cooperate with other mechanisms for detecting and avoiding attacks in the IoT.

Acronyms

3GPP:	3rd Generation Partnership Project
AES:	Advanced encryption standard
AKA:	Authentication and key agreement protocol
AMACs:	Aggregate message authentication codes
AVISPA:	Automated Validation of Internet Security Protocols and Application
BAN-logic:	Burrows-Abadi-Needham Logic
BTS:	Base Transceiver Station
DoS:	Denial of Service attack
ECC:	Elliptic Curve Cryptography
ECDH:	Elliptic Curve Diffie-Hellman
GPS:	Global Positioning System
HANs:	Home area networks
HMAC:	Keyed-hashing for message authentication
HSLV:	Heavy signing light verification
IBC:	ID-based cryptography
IIoT:	Industrial Internet of Things
IoBT:	Internet of biometric things
IoE:	Internet of Energy
IoS:	Internet of Sensors
IoT:	Internet of Things
IoV:	Internet of Vehicles
LSHV:	Light signing heavy verification
M2M:	Machine to Machine Communications
MAC:	Message Authentication Code
MD5:	Message Digest 5
MHT:	Merkle Hash Tree
MITM:	Man-in-the-middle attack
MS:	Mobile Station
MTC:	Machine-type Communication
PKI:	Public Key Infrastructure
PMIP:	Proxy Mobile IP
RFID:	Radio Frequency Identification
RSUs:	Road Side Units
SDON:	Software Defined Optical Network
SHA:	Secure Hash Algorithm
SIoV:	Social Internet of Vehicles
VANET:	Vehicular ad hoc network
WiMAX:	Worldwide Interoperability for Microwave Access
WoT:	Web of Things
WSN:	Wireless Sensor Network.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Evans, "The internet of things, How the Next Evolution of the Internet is Changing Everything," *Whitepaper, Cisco Internet Business Solutions Group (IBSG)*, vol. 1, pp. 1–12, 2011, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[2] IBM IoT, http://www.ibm.com/internet-of-things/.

[3] "Watson IoT," http://www.ibm.com/internet-of-things/learn/library/what-is-watson-iot/.

[4] "Softlayer," http://www.softlayer.com/.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[6] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[7] A. Aijaz and A. H. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: a protocol stack perspective," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 103–112, 2015.

[8] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT '14)*, pp. 241–246, March 2014.

[9] L. A. Maglaras and D. Katsaros, "Social clustering of vehicles based on semi-Markov processes," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 318–332, 2016.

[10] L. A. Maglaras and D. Katsaros, "Distributed clustering in vehicular networks," in *Proceedings of the 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2012*, pp. 593–599, esp, October 2012.

[11] "ARTEMIS-project," http://www.artemis-ioe.eu/.

[12] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: a practical approach," *IEEE Communications Magazine*, vol. 50, no. 6, pp. 134–143, 2012.

[13] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[14] J. Cooper and A. James, "Challenges for database management in the internet of things," *IETE Technical Review*, vol. 26, no. 5, pp. 320–329, 2009.

[15] R. H. Weber, "Internet of Things , New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[16] C. M. Medaglia and A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," in *The Internet of Things*, pp. 389–395, Springer New York, NY, USA, 2010.

[17] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 168–174, 2010.

[18] A. A. Shidhani and V. C. M. Leung, "Secure and efficient multi-hop mobile IP registration scheme for MANET-internet integrated architecture," in *Proceedings of the IEEE Wireless Communications and Networking Conference 2010, WCNC 2010*, aus, April 2010.

[19] T.-H. Chen and W.-K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI Journal*, vol. 32, no. 5, pp. 704–712, 2010.

[20] R. Fan, L.-D. Ping, J.-Q. Fu, and X.-Z. Pan, "A secure and efficient user authentication protocol for two-tiered wireless sensor networks," in *Proceedings of the 2010 2nd Pacific-Asia Conference on Circuits, Communications and System, PACCS 2010*, pp. 425–428, chn, August 2010.

[21] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *Proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '10)*, pp. 600–606, October 2010.

[22] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 4, pp. 361–371, 2010.

[23] H.-F. Huang, Y.-F. Chang, and C.-H. Liu, "Enhancement of two-factor user authentication in wireless sensor networks," in *Proceedings of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2010*, pp. 27–30, deu, October 2010.

[24] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[25] Y.-L. Huang, C.-Y. Shen, and S. W. Shieh, "S-AKA: a provable and secure authentication key agreement protocol for UMTS networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, pp. 4509–4519, 2011.

[26] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 431–436, 2011.

[27] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. L. Boudec, "Adaptive message authentication for multi-hop networks," in *Proceedings of the 2011 8th International Conference on Wireless On-Demand Network Systems and Services, WONS 2011*, pp. 96–103, ita, January 2011.

[28] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 686–696, 2011.

[29] "I. standard 802.16m 2011," Tech. Rep., Air interface for broadband wireless access systems - Amendment 3: advanced air interface.

[30] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

[31] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[32] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 1017–1022, Anaheim, Calif, USA, December 2012.

[33] Y.-W. Chen, J.-T. Wang, K.-H. Chi, and C.-C. Tseng, "Group-based authentication and key agreement," *Wireless Personal Communications*, vol. 62, no. 4, pp. 965–979, 2012.

[34] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, “A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks,” *IEEE Communications Letters*, vol. 16, no. 11, pp. 1744–1747, 2012.

[35] R. Sule, R. S. Katti, and R. G. Kavasseri, “A variable length fast message authentication code for secure communication in smart grids,” in *Proceedings of the 2012 IEEE Power and Energy Society General Meeting, PES 2012*, usa, July 2012.

[36] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, “A dynamic password-based user authentication scheme for hierarchical wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.

[37] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, “LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks,” in *Proceedings of the IEEE Global Communications Conference (GLOBECOM ’13)*, pp. 832–837, December 2013.

[38] C. Lai, H. Li, R. Lu, and X. Shen, “SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks,” *Computer Networks*, vol. 57, no. 17, pp. 3492–3510, 2013.

[39] S. Cespedes, S. Taha, and X. Shen, “A multihop-authenticated proxy mobile IP scheme for asymmetric VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3271–3286, 2013.

[40] A. Wasef and X. S. Shen, “EMAP: Expedite message authentication protocol for vehicular ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, 2013.

[41] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

[42] C.-T. Li, C.-Y. Weng, and C.-C. Lee, “An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks,” *Sensors*, vol. 13, no. 8, pp. 9589–9603, 2013.

[43] Q. Jiang, J. Ma, G. Li, and L. Yang, “An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks,” *Wireless Personal Communications*, vol. 68, no. 4, pp. 1477–1491, 2013.

[44] F. Wen, W. Susilo, and G. Yang, “A secure and effective anonymous user authentication scheme for roaming service in global mobility networks,” *Wireless Personal Communications*, vol. 73, no. 3, pp. 993–1004, 2013.

[45] M. Turkanovic and M. Holbl, “An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks,” *Elektronika ir Elektrotechnika*, vol. 19, no. 6, pp. 109–116, 2013.

[46] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, “SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks,” in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 1011–1016, aus, June 2014.

[47] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, “CPAL: A conditional privacy-preserving authentication with access linkability for roaming service,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 46–57, 2014.

[48] A. C.-F. Chan and J. Zhou, “Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.

[49] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, “An efficient Merkle-tree-based authentication scheme for smart grid,” *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.

[50] Y. Choi, D. Lee, and J. Kim, “Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography,” *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.

[51] M. Turkanović, B. Brumen, and M. Hölbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,” *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[52] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, “Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response,” *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.

[53] X. Sun, S. Men, C. Zhao, and Z. Zhou, “A security authentication scheme in machine-to-machine home network service,” *Security and Communication Networks*, vol. 8, no. 16, pp. 2678–2686, 2015.

[54] C. Lai, R. Lu, and D. Zheng, “SGSA: Secure group setup and anonymous authentication in platoon-based vehicular cyber-physical systems,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 9204, pp. 274–283, 2015.

[55] T. W. Chim, S.-M. Yiu, V. O. Li, L. C. Hui, and J. Zhong, “PRGA: Privacy-Preserving Recording amp; Gateway-Assisted Authentication of Power Usage Information for Smart Grid,” *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, 2015.

[56] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, “A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity,” *Security and Communication Networks*, vol. 9, no. 15, pp. 2643–2655, 2016.

[57] D. He, N. Kumar, and N. Chilamkurti, “A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks,” *Information Sciences*, vol. 321, Article ID 11403, pp. 263–277, 2015.

[58] S. Shin, H. Yeh, and K. Kim, “An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks,” *Peer-to-Peer Networking and Applications*, vol. 8, no. 4, pp. 674–683, 2015.

[59] G. Prosanta and T. Hwang, “Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks,” *IEEE Systems Journal*, vol. PP, no. 99, 2015.

[60] M. S. Farash, S. A. Chaudhry, M. Heydari, S. M. Sajad Sadough, S. Kumari, and M. K. Khan, “A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security,” *International Journal of Communication Systems*, vol. 30, no. 4, Article ID e3019, 2017.

[61] C. Lai, R. Lu, D. Zheng, H. Li, and X. Sherman, “GLARM: group-based lightweight authentication scheme for resource-constrained machine to machine communications,” *Computer Networks*, vol. 99, pp. 66–81, 2016.

[62] D. Chen, N. Zhang, and Z. Qin, “S2M: a lightweight acoustic fingerprints based wireless device authentication protocol,” *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[63] J. Shao, X. Lin, R. Lu, and C. Zuo, “A Threshold Anonymous Authentication Protocol for VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[64] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-Based Authentication for Vehicle-to-Vehicle Communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 71–83, 2016.

[65] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed Aggregate Privacy-Preserving Authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2016.

[66] S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal, "Vehicle authentication via monolithically certified public key and attributes," *Wireless Networks*, vol. 22, no. 3, pp. 879–896, 2016.

[67] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," *Computers Electrical Engineering*, vol. 52, pp. 114–124, 2016.

[68] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, vol. 63, pp. 56–75, 2016.

[69] Y. Chung, S. Choi, Y. S. Lee, N. Park, and D. Won, "An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks," *Sensors*, vol. 16, no. 10, article no. 1653, 2016.

[70] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, part 1, pp. 58–80, 2016.

[71] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Transactions on Industrial Electronics*, 2016.

[72] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 223–244, 2016.

[73] C.-C. Chang and H.-D. Le, "A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357–366, 2016.

[74] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[75] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[76] S. Kumari, A. K. Das, M. Wazid et al., "On the design of a secure user authentication and key agreement scheme for wireless sensor networks," *Concurrency Computation*, 2016.

[77] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," *International Journal of Network Management*, vol. 27, no. 3, Article ID e1937, 2017.

[78] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "Data quality in internet of things: A state-of-the-art survey," *Journal of Network and Computer Applications*, vol. 73, pp. 57–81, 2016.

[79] Q. Yongrui, Q. Z. Sheng, N. J. G. Falkner, S. Dustdar, H. Wang, and A. V. Vasilakos, "When things matter: a survey on data-centric internet of things," *Journal of Network and Computer Applications*, vol. 64, pp. 137–153, 2016.

[80] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2546–2590, 2016.

[81] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for internet of things," in *Recent Trends in Wireless and Mobile Networks*, vol. 162 of *Communications in Computer and Information Science*, pp. 288–296, Springer, Berlin, Germany, 2011.

[82] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," in *Proceedings of the 13th International Conference on Collaboration Technologies and Systems (CTS '12)*, pp. 21–26, Denver, Colo, USA, May 2012.

[83] T. Teixeira, S. Hachem, V. Issarny, and N. Georgantas, "Service oriented middleware for the internet of things: A perspective (invited paper)," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 6994, pp. 220–229, 2011.

[84] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.

[85] A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[86] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges," *IEEE Wireless Communications Magazine*, vol. 23, no. 5, pp. 10–16, 2016.

[87] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 58–67, 2011.

[88] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: a survey," in *Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM '11)*, pp. 16–21, September 2011.

[89] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things," *Computers Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[90] C. C. Aggarwal, N. Ashish, and A. Sheth, "The Internet of Things: A Survey from the Data-Centric Perspective," in *Managing and Mining Sensor Data*, pp. 383–428, Springer US, Boston, MA, 2013.

[91] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the internet of things: a survey," *IEEE Access*, vol. 4, pp. 5591–5606, 2016.

[92] P. Rawat, K. D. Singh, and J. M. Bonnin, "Cognitive radio for M2M and Internet of Things: A survey," *Computer Communications*, vol. 94, pp. 1–29, 2016.

[93] D. Bandyopadhyay and J. Sen, "Internet of things: applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[94] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[95] Z. G. Sheng, S. S. Yang, Y. F. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," *IEEE Wireless Communications Magazine*, vol. 20, no. 6, pp. 91–98, 2013.

[96] I. Ishaq, D. Carels, G. Teklemariam et al., "IETF standardization in the field of the internet of things (IoT): a survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, 2013.

[97] M. R. Palattella, N. Accettura, X. Vilajosana et al., "Standardized protocol stack for the internet of (important) things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[98] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, 2014.

[99] M. C. Domingo, "An overview of the internet of things for people with disabilities," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 584–596, 2012.

[100] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[101] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on internet of things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[102] Z. Bi, L. D. Xu, and C. Wang, "Internet of things for enterprise systems of modern manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1537–1546, 2014.

[103] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: state of the art," pp. 55–75, 2016.

[104] D. Zhang, L. T. Yang, and H. Huang, "Searching in Internet of Things: Vision and challenges," in *Proceedings of the 9th IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA 2011*, pp. 201–206, kor, May 2011.

[105] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12)*, pp. 648–651, Hangzhou, China, March 2012.

[106] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[107] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[108] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[109] S. Chabridon, R. Laborde, T. Desprats, A. Oglaza, P. Marie, and S. M. Marquez, "A survey on addressing privacy together with quality of context for context management in the Internet of Things," *Annals of Telecommunications-Annales des Télécommunications*, vol. 69, no. 1-2, pp. 47–62, 2014.

[110] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[111] W. Xie, Y. Tang, S. Chen, Y. Zhang, and Y. Gao, "Security of Web of Things: A Survey (Short Paper)," in *Advances in Information and Computer Security*, vol. 9836 of *Lecture Notes in Computer Science*, pp. 61–70, Springer International Publishing, Cham, 2016.

[112] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: a standardization perspective," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265–275, 2014.

[113] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[114] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[115] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC '15)*, pp. 1–6, IEEE, San Francisco, Calif, USA, June 2015.

[116] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, article no. 1181, pp. 17–31, 2015.

[117] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, 2016.

[118] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Research*, vol. 26, no. 2, pp. 337–359, 2016.

[119] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 198–213, 2016.

[120] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012*, pp. 1282–1285, chn, April 2012.

[121] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 72–83, 2015.

[122] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[123] B. Guo, D. Zhang, Z. Wang, Z. Yu, and X. Zhou, "Opportunistic IoT: exploring the harmonious interaction between human and the internet of things," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1531–1539, 2013.

[124] A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, "The cluster between internet of things and social networks: Review and research challenges," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 206–215, 2014.

[125] L. Maglaras, A. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, "Social Internet of Vehicles for Smart Cities," *Journal of Sensor and Actuator Networks*, vol. 5, no. 1, p. 3, 2016.

[126] H.-D. Ma, "Internet of things: objectives and scientific challenges," *Journal of Computer Science and Technology*, vol. 26, no. 6, pp. 919–924, 2011.

[127] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the 1st ACM Mobile Cloud Computing Workshop, MCC 2012*, pp. 13–15, fin, August 2012.

[128] A. Botta, W. De Donato, V. Persico, and A. Pescape, "On the integration of cloud computing and internet of things," in *Proceedings of the 2nd International Conference on Future Internet of Things and Cloud (FiCloud '14)*, pp. 23–30, Barcelona, Spain, August 2014.

[129] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things—a survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[130] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[131] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[132] J. Liu, H. Shen, and X. Zhang, "A survey of mobile crowdsensing techniques: A critical component for the internet of things," in *Proceedings of the 25th International Conference on Computer Communications and Networks, ICCCN 2016*, usa, August 2016.

[133] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of things: a review of surveys based on context aware intelligent services," *Sensors*, vol. 16, no. 7, article 1069, 2016.

[134] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, pp. 99–117, 2016.

[135] C. Tsai, C. Lai, M. Chiang, and L. T. Yang, "Data mining for internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 77–97, 2014.

[136] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos, and X. Rong, "Data mining for the internet of things: Literature review and challenges," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 431047, 2015.

[137] H. Zhu, X. Lin, Y. Zhang, and R. Lu, "Duth: A user-friendly dual-factor authentication for Android smartphone devices," *Security and Communication Networks*, vol. 8, no. 7, pp. 1213–1222, 2015.

[138] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis," in *Proceedings of the IEEE PES Innovative Smart Grid Technologies (ISGT '12)*, pp. 1–8, IEEE, January 2012.

[139] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *Proceedings of the IEEE Power and Energy Society'sInnovative Smart Grid Technologies Asia 2011 Conference,ISGT Asia 2011*, aus, November 2011.

[140] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving authentication scheme for smart grid network," in *Proceedings of the 2011 IEEE 2nd International Conference on Smart Grid Communications, SmartGridComm 2011*, pp. 196–201, bel, October 2011.

[141] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "Towards a light-weight message authentication mechanism tailored for Smart Grid communications," in *Proceedings of the 2011 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2011*, pp. 1018–1023, chn, April 2011.

[142] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629–640, 2014.

[143] M. Jan, P. Nanda, M. Usman, and X. He, "PAWN: A payload-based mutual authentication scheme for wireless sensor networks," *Concurrency Computation*, 2016.

[144] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol. 54, pp. 147–169, 2017.

[145] X. Sun, X. Wu, C. Huang, Z. Xu, and J. Zhong, "Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks," *Ad Hoc Networks*, vol. 37, pp. 324–336, 2016.

[146] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, pp. 1–20, 2016.

[147] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 16, pp. 3670–3687, 2016.

[148] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers & Electrical Engineering*, 2016.

[149] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2007.

[150] J. Katz and A. Y. Lindell, "Aggregate Message Authentication Codes," in *Topics in Cryptology CT-RSA*, pp. 155–169, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[151] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.

[152] E. Barker, L. Chen, A. Roginsky, and M. Smid, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," National Institute of Standards and Technology NIST SP 800-56Ar2, 2013.

[153] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography*, vol. 2595, pp. 310–324, Springer, Berlin, Germany, 2003.

[154] P. Chown, "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)," RFC Editor RFC3268, 2002.

[155] J. Y. Hwang, S. Lee, B.-H. Chung, H. S. Cho, and D. Nyang, "Group signatures with controllable linkability for dynamic membership," *Information Sciences*, vol. 222, pp. 761–778, 2013.

[156] T. Schmidt, M. Waehlisch, and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains," RFC Editor RFC6224, 2011.

[157] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," in *Advances in Cryptology*, pp. 335–338, Springer Berlin Heidelberg, Berlin, Heidelberg, 1984.

[158] T. H. Cormen, C. E. Leiserson, R. Rivest, and C. Stein, *Introduction to Algorithms*, The MIT Press, 2009.

[159] D. Chaum and E. van Heyst, "Group Signatures," in *Advances in Cryptology — EUROCRYPT '91*, vol. 547 of *Lecture Notes in Computer Science*, pp. 257–265, Springer Berlin Heidelberg, Berlin, Heidelberg, 1991.

[160] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology—CRYPTO 2004*, vol. 3152 of *Lecture Notes in Computer Science*, pp. 41–55, Springer, Berlin, Germany, 2004.

[161] R. C. Merkle, R. Charles et al., "Secrecy, authentication, and public key systems".

[162] A. Perrig, R. Canetti, D. Song, U. C. Berkeley, D. Fountain, and I. B. M. T. J. Watson, "Efficient and Secure Source Authentication for Multicast," in *Proceedings of the Internet Society Network and Distributed System Security Symposium*, pp. 35–46, 2001.

[163] "IEEE Std 1609.2-2013," IEEE standard for wireless access in vehicular environments - Security services for applications and management messages.

[164] E. Kiltz and K. Pietrzak, “Leakage resilient ElGamal encryption,” in *Advances in Cryptology—ASIACRYPT ’10*, vol. 6477 of *Lecture Notes in Computer Science*, pp. 595–612, Springer, Berlin, Germany, 2010.

[165] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *Proceedings of the the 11th ACM conference*, p. 168, Washington DC, USA, October 2004.

[166] D. Bleichenbacher and A. May, “New attacks on RSA with small secret CRT-exponents,” in *Public key cryptography-PKC*, vol. 3958, pp. 1–13, Springer, Berlin, 2006.

[167] D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[168] B. Li, Z. Wang, and D. Huang, “An Efficient and Anonymous Attribute-Based group setup scheme,” in *Proceedings of the 2013 IEEE Global Communications Conference, GLOBECOM 2013*, pp. 861–866, usa, December 2013.

[169] H. Krawczyk, M. Bellare, and R. Canetti, “RFC2104 - HMAC: Keyed-hashing for message authentication,” Tech. Rep., 1997, arXiv:arXiv:1011.1669v3.

[170] L. Reyzin and N. Reyzin, “Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying,” in *Information Security and Privacy*, vol. 2384 of *Lecture Notes in Computer Science*, pp. 144–153, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[171] R. Rivest, “The MD5 Message-Digest Algorithm,” RFC Editor RFC1321, 1992.

[172] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, vol. 17, no. 4, pp. 297–319, 2004.

[173] L. Harn, “Batch verifying multiple RSA digital signatures,” *IEEE Electronics Letters*, vol. 34, no. 12, pp. 1219-1220, 1998.

[174] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps,” in *Advances in cryptology—EUROCRYPT 2003*, vol. 2656 of *Lecture Notes in Comput. Sci.*, pp. 416–432, Springer, Berlin, 2003.

[175] J. Jonsson and B. Kaliski, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,” RFC Editor RFC3447, 2003.

[176] P. Jones, “US secure hash algorithm 1 (SHA1) RFC 3174,” Tech. Rep., 2001, http://rsync.tools.ietf.org/html/rfc3174.

[177] S. Turner and L. Chen, “Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms,” RFC Editor RFC6151, 2011.

[178] D. R. Stinson, *Cryptography: theory and practice*, CRC press, 2002.

[179] H. Nicanfar and V. C. M. Leung, “EIBC: Enhanced identity-based cryptography, a conceptual design,” in *Proceedings of the 2012 6th IEEE International Systems Conference, SysCon 2012*, pp. 179–185, can, March 2012.

[180] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in *Advances in Cryptology—CRYPTO 2001*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, 2001.

[181] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Advances in Cryptology—EUROCRYPT ’99*, vol. 1592, pp. 223–238, Springer, 1999.

[182] A. Kumar, J. JimXu, and J. Wang, “Space-code bloom filter for efficient per-flow traffic measurement,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 12, pp. 2327–2339, 2006.

[183] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*, CRC Press, Boca Raton, Fla, USA, 2003.

[184] S. Han and E. Chang, “Chaotic map based key agreement with/out clock synchronization, Chaos,” *Solitons & Fractals*, vol. 39, no. 3, pp. 1283–1289, 2009.

[185] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.

[186] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,” *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

[187] A. T. B. Jin, D. N. C. Ling, and A. Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,” *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[188] R. Dutta, S. Mukhopadhyay, and T. Dowling, “Enhanced Access Polynomial Based Self-healing Key Distribution,” in *Security in Emerging Wireless Communication and Networking Systems*, vol. 42 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 13–24, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[189] D. Hankerson, S. Vanstone, and A. J. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, New York, NY, USA, 2004.

[190] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1070–1081, 2015.

[191] B. Blanchet, V. Cheval, X. Allamigeon, and B. Smyth, *Proverif: Cryptographic protocol verifier in the formal model*, 2010.

[192] M. Abadi and A. D. Gordon, “A calculus for cryptographic protocols,” in *Proceedings of the the 4th ACM conference*, pp. 36–47, Zurich, Switzerland, April 1997.

[193] “NXP, ATOP datasheet,” http://www.nxp.com/documents/leaflet/939775016910.pdf.

[194] “AVISPA-Automated Validation of Internet Security Protocols,” http://www.avispa-project.org.

[195] M. Burrows, M. Abadi, and R. Needham, “Logic of authentication,” *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[196] D. Dolev and A. C. Yao, “On the security of public key protocols,” *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[197] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, “An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks,” *Security and Communication Networks*, vol. 9, no. 13, pp. 2070–2092, 2016.

[198] G. Chandrasekaran, J.-A. Francisco, V. Ganapathy, M. Gruteser, and W. Trappe, “Detecting identity spoofs in IEEE 802.11e wireless networks,” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM ’09)*, pp. 1–6, IEEE, December 2009.

[199] N. Patwari and S. K. Kasera, “Robust location distinction using temporal link signatures,” in *Proceedings of the the 13th annual ACM international conference*, p. 111, Montreal, Québec, Canada, September 2007.

[200] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “A physical-layer technique to enhance authentication for mobile terminals,” in *Proceedings of the IEEE International Conference on Communications, ICC 2008*, pp. 1520–1524, chn, May 2008.

[201] J. Xiong and K. Jamieson, "SecureArray: improving wifi security with fine-grained physical-layer information in," in *Proceedings of the 19th annual international conference on Mobile computing networking - MobiCom 13*, pp. 441-10, New York, New York, USA, 2013.

[202] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC 2008*, pp. 2543–2548, usa, April 2008.

[203] I. standard 802.16m 2011, Air interface for broadband wireless access systems - Amendment 3: advanced air interface.

[204] C.-M. Huang and J.-W. Li, "A cluster-chain-based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture," *Wireless Communications and Mobile Computing*, vol. 9, no. 10, pp. 1387–1401, 2009.

[205] J. Jeong, Y. C. Min, and H. Choo, "Integrated OTP-based user authentication scheme using smart cards in home networks," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences 2008, HICSS*, usa, January 2008.

[206] R. Baldessari, W. Zhang, A. Festag, and L. Le, "A MANET-centric Solution for the Application of NEMO in VANET Using Geographic Routing," in *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, p. 12, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[207] "ISO/IEC is 9798-3, Entity authentication mechanisms, part 3: Entity authentication using asymmetric techniques".

[208] H. Krawczyk, "SIGMA: The SIGn-and-MAc Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols," in *Proceedings of the Annual International Cryptology Conference*, vol. 2729, pp. 400–425.

[209] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *Proceedings of the 28th Conference on Computer Communications, IEEE INFOCOM 2009*, pp. 1233–1241, bra, April 2009.

[210] H. Gharavi and B. Hu, "Multigate communication network for smart grid," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1028–1045, 2011.

[211] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 730831, 2013.

[212] E. Borgia, "The internet of things vision: key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[213] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[214] Y. YIN, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," *Journal of Industrial Information Integration*, vol. 1, pp. 3–13, 2016.

[215] M. A. Ferrag, N. Chekkai, and M. Nafa, "Securing Embedded Systems: Cyberattacks, Countermeasures, and Challenges," in *Securing Cyber-Physical Systems*, pp. 279–304, CRC Press, 2015.

[216] M. A. Ferrag, M. Nafa, and S. Ghanemi, "Security and privacy in mobile Ad Hoc social networks," *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*, pp. 222–243, 2013.

[217] M. Ferrag, M. Nafa, and S. Ghanemi, "Security and Privacy for Routing Protocols in Mobile Ad Hoc Networks," in *Security for Multihop Wireless Networks*, pp. 19–42, CRC Press, 2014.

[218] , *Security Solutions and Applied Cryptography in Smart Grid Communications*, M. A. Ferrag and A. Ahmim, Eds., IGI Global, 2017.

[219] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "A Survey on Privacy-preserving Schemes for Smart Grid Communications," http://arxiv.org/abs/1611.07722.

[220] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for Ad Hoc Social Networks: A survey," *IEEE Communications Surveys & Tutorials*, pp. 1-1.

[221] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," RFC Editor RFC3776, 2004.

[222] D. Coppersmith, "Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243–250, 1994.

[223] C. P. Schnorr and M. Jakobsson, "Security of signed ElGamal encryption," in *Advances in cryptology—ASIACRYPT 2000*, vol. 1976 of *Lecture Notes in Computer Science*, pp. 73–89, Springer, Berlin, Germany, 2000.

[224] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC Editor RFC5213, 2008.

[225] I. Rivin, "Symmetrized Chebyshev polynomials," *Proceedings of the American Mathematical Society*, vol. 133, no. 5, pp. 1299–1305, 2005.

[226] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," *Computers & Security*, vol. 21, no. 4, pp. 372–375, 2002.

[227] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, article 25, 2013.

[228] *G. T. V12.5.0, 3GPP System Architecture Evolution (SAE)*, Security architecture.

[229] A. Esfahani, G. Mantas, R. Matischek et al., "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," *IEEE Internet of Things Journal*, pp. 1-1.

[230] C. Zhao, L. Huang, Y. Zhao, and X. Du, "Secure machine-type communications toward LTE heterogeneous networks," *IEEE Wireless Communications Magazine*, vol. 24, no. 1, pp. 82–87, 2017.

[231] Y. Qiu and M. Ma, "A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN networks," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, 2016.

[232] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," *Future Generation Computer Systems*, 2016.

[233] S. H. Islam, P. Vijayakumar, M. Z. Bhuiyan, R. Amin, V. R. M., and B. Balusamy, "A Provably Secure Three-factor Session Initiation Protocol for Multimedia Big Data Communications," *IEEE Internet of Things Journal*, pp. 1-1.

[234] R. Amin, R. Sherratt, D. Giri, S. Islam, and M. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 1, pp. 53–61, 2017.

[235] M. A. Ferrag and A. Ahmim, "ESSPR: an efficient secure routing scheme based on searchable encryption with vehicle

proxy re-encryption for vehicular peer-to-peer social network," *Telecommunication Systems*, pp. 1–23, 2017.

[236] N. Saxena, B. J. Choi, and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907–921, 2016.

[237] *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, National Institute of Standards and Technology, https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf.

[238] J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey," *Ad Hoc Networks*, vol. 24, pp. 264–287, 2015.

[239] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol. 27, pp. 159–194, 2015.

[240] K. Grover and A. Lim, "A survey of broadcast authentication schemes for wireless networks," *Ad Hoc Networks*, vol. 24, pp. 288–316, 2015.

[241] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.

[242] C.-Y. Chen and H.-C. Chao, "A survey of key distribution in wireless sensor networks," *Security and Communication Networks*, vol. 7, no. 12, pp. 2495–2508, 2014.

[243] M. A. Simplicio Jr., B. T. De Oliveira, C. B. Margi, P. S. L. M. Barreto, T. C. M. B. Carvalho, and M. Näslund, "Survey and comparison of message authentication solutions on wireless sensor networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1221–1236, 2013.

[244] M. A. Ferrag, M. Nafa, and S. Ghanemi, "EPSA: An efficient and privacy-preserving scheme against wormhole attack on reactive routing for mobile ad hoc social networks," *International Journal of Security and Networks*, vol. 11, no. 3, pp. 107–125, 2016.

[245] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '00)*, vol. 2, IEEE, January 2000.

[246] L. B. Oliveira, A. Ferreira, M. A. Vilaça et al., "SecLEACH-on the security of clustered sensor networks," *Signal Processing*, vol. 87, no. 12, pp. 2882–2895, 2007.

[247] A. K. Das, "A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1377–1404, 2015.

[248] S. G. Yoo, K. Y. Park, and J. Kim, "A security-performance-balanced user authentication scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 382810, 11 pages, 2012.

[249] D.-Z. Sun, J.-X. Li, Z.-Y. Feng, Z.-F. Cao, and G.-Q. Xu, "ON the security and improvement of a two-factor user authentication scheme in wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 895–905, 2013.

[250] J. Nam, M. Kim, J. Paik, Y. Lee, and D. Won, "A provably-secure ECC-based authentication scheme for wireless sensor networks," *Sensors*, vol. 14, no. 11, pp. 21023–21044, 2014.

[251] A. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems*, vol. 30, no. 1, Article ID e2933, 2017.

[252] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei, "A dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol. 1, pp. 244–251, Taichung, Taiwan, June 2006.

[253] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[254] P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 17, no. 2, pp. 498–503, 2017.

[255] C. Benzaid, K. Lounis, A. Al-Nemrat, N. Badache, and M. Alazab, "Fast authentication in wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 362–375, 2016.

[256] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," *Computer Communications*, vol. 31, no. 4, pp. 659–667, 2008.

[257] X. Fan and G. Gong, "Accelerating signature-based broadcast authentication for wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 4, pp. 723–736, 2012.

[258] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4255–4271, 2016.

[259] M. Nitti, R. Girau, A. Floris, and L. Atzori, "On adding the social dimension to the Internet of Vehicles: Friendship and middleware," in *Proceedings of the 2014 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2014*, pp. 134–138, mda, May 2014.

[260] T. H. Luan, R. Lu, X. Shen, and F. Bai, "Social on the road: enabling secure and efficient social networking on highways," *IEEE Wireless Communications Magazine*, vol. 22, no. 1, pp. 44–51, 2015.

[261] A. Gantman and D. M. Jacobson, *Secure software authentication and verification*, 2015.

[262] M. M. Haghighi and M. S. Zamani, "Soft IP protection: An active approach based on hardware authentication," in *Proceedings of the 24th Iranian Conference on Electrical Engineering, ICEE 2016*, pp. 1049–1054, irn, May 2016.

[263] H. U. D. Z. C. L. I. U. Peng, "RFID Middleware Authentication Protocol Design Based on Symmetrical Cryptographic Algorithm," *Computer & Digital Engineering*, vol. 3, p. 36, 2013.

[264] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[265] D. Shah and V. Haradi, "IoT Based Biometrics Implementation on Raspberry Pi," in *Proceedings of the 7th International Conference on Communication, Computing and Virtualization, ICCCV 2016*, pp. 328–336, ind, February 2016.

[266] N. Karimian, P. A. Wortman, and F. Tehranipoor, "Evolving authentication design considerations for the Internet of biometric things (IoBT)," in *Proceedings of the 2016 International Conference on Hardware/Software Codesign and System Synthesis, CODES+ISSS 2016*, usa, October 2016.

[267] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, Discovery, and Authentication for the Internet of Things," in *Computer Security – ESORICS 2016*, vol. 9879 of *Lecture Notes in Computer*

Science, pp. 301–319, Springer International Publishing, Cham, 2016.

[268] P. Schulz, M. Matthe, H. Klessig et al., “Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture,” *IEEE Communications Magazine*, vol. 55, no. 2, pp. 70–78, 2017.

[269] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, *Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes*, http://arxiv.org/abs/1708.04027.

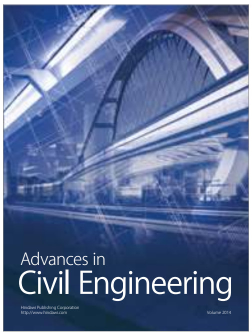
Journal of
Engineering

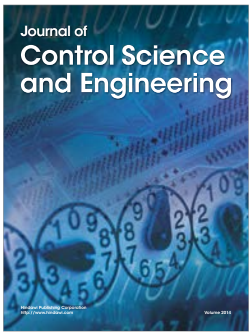
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

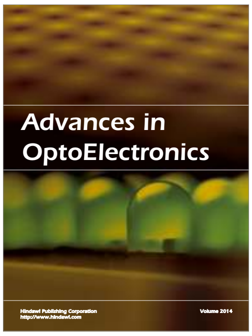
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

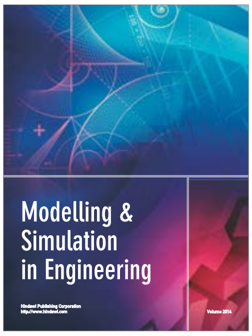
Journal of
Robotics

Journal of
Electrical and Computer Engineering


Advances in
OptoElectronics

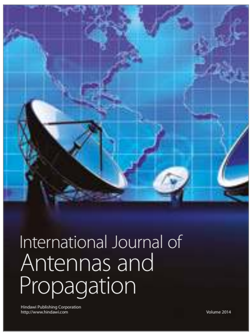
VLSI Design

International Journal of
Navigation and Observation

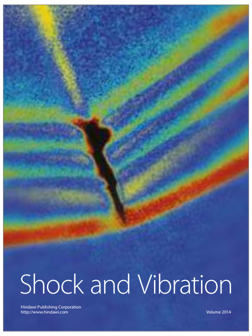

Modelling &
Simulation
in Engineering

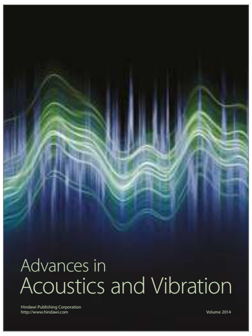
International Journal of
Aerospace Engineering

International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration