Open Access
Published Online First: Suppl. November 2022

Baghdad Science Journal
2022, 19(6): 1430-1444

P-ISSN: 2078-8665
E-ISSN: 2411-7986

DOI: https://dx.doi.org/10.21123/bsj.2022.7312

IPv6 Security Issues: A Systematic Review Following PRISMA Guidelines

Shubair A. Abdullah *[1]

Ahmed A. Al Ashoor [2]

[1]Sultan Qaboos University, Muscat, Oman.
[2]University of Basrah, Basrah, Iraq.
[*]Corresponding author: shubair@squ.edu.om
E-mail addresses: shubair@squ.edu.om , ahmed.ashur@uobasrah.edu.iq

Received 10/4/2022, Accepted 4/8/2022, Published Online First 25/11/2022, Published 5/12/2022

Abstract:

Since Internet Protocol version 6 is a new technology, insecure network configurations are inevitable. The researchers contributed a lot to spreading knowledge about IPv6 vulnerabilities and how to address them over the past two decades. In this study, a systematic literature review is conducted to analyze research progress in IPv6 security field following the Preferred Reporting Items for the Systematics Review and Meta-Analysis (PRISMA) method. A total of 427 studies have been reviewed from two databases, IEEE and Scopus. To fulfil the review goal, several key data elements were extracted from each study and two kinds of analysis were administered: descriptive analysis and literature classification. The results show positive signs of the research contributions in the field, and generally, they could be considered as a reference to explore the research of in the past two decades in IPv6 security field and to draw the future directions. For example, the percentage of publishing increased from 147 per decade from 2000-2010 to 330 per decade from 2011 to 2020 which means that the percentage increase was 124%. The number of citations is another key finding that reflects the great global interest in research devoted to IPv6 security issues, as it was 409 citations in the decade from 2000-2010, then increased to 1643 citations during the decade from 2011 to 2020, that is, the percentage increase was 302%.

Keywords: IPv6, IPv6 Deployment, IPv6 Security, PRISMA Guidelines, Systematic Review.

Introduction:

On 3rd of February 2011, the Internet Assigned Numbers Authority (IANA) announced allocation of the last batch of IPv4 address blocks to the Regional Internet Registries (RIRs), thus running out of the free pool of available IPv4 addresses in the RIR's designated areas can become a reality at any time [1]. Due to the recent exponential growth of the Internet that leads to the imminent depletion of IPv4 address space, the importance of IPv6 to the future of the Internet is now without question. The IPv6 protocol is based on 128-bit addresses and it can provide roughly 3.4×1038 unique addresses. Not only does this huge number of IP addresses solve the address scarcity in IPv4, it also facilitates the transition to the Internet of Things (IoT), fifth generation cellular (5G), and cloud-based services [2]. For instance, the IoT technology refers to billions of devices around the world, such as smart refrigerators, smart watches, smart fire alarm, smart door lock, smart bicycle, medical sensors, fitness trackers, etc., connected to the Internet with ability of collecting and sharing data [3]. All of these devices need IP addresses to communicate, and only IPv6 technology is able to provide such a huge number of addresses. In addition to the galore of addresses, IPv6 protocol includes many new features that make it an excellent alternative to IPv4, such as new header format, large address space, stateless and stateful address configuration, the mandatory of using IPsec, and new protocol for neighboring node interaction [4]. IPv4 must eventually be replaced with IPv6, despite the existence of some solutions, such as reusing and recycling unused IPv4 addresses by the ISPs and using the network address translation devices that allow using IPv4 addresses privately behind the ISPs router.

The adoption of IPv6 is increasing significantly in recent years. Google is continuously measuring the availability of IPv6 traffic initiated by Google users. According to their IPv6 statistics, the percentage of users accessing Google via IPv6 as of November 2020 is 30%, and more than 25 countries around the world deliver 20% or above of their traffic using the new protocol [5]. Although these numbers clearly indicate that the deployment of IPv6 has become a priority for many organizations and countries, the global network communities are still far from achieving the ambitious goal of IPv6 deployment. Since the IPv6 is a new technology to be deployed in currently established IT environments within the enterprises, it is considered an important financial, administrative and technical challenges for these enterprises. The IPv6 protocol, of course, brings new security threats, and this is a constant concern for enterprises when they start deploying IPv6. IPv6 protocol has some enhancements that increase the level of security, such as the mandatory use of IPSec, Authentication Header (AH), Encapsulating Security Payload (ESP), large address space, and neighbor discovery. However, the IT administrations, network administrators, and network security researchers need more practical guides and technical tutorials to review and/or update IPv4 security and maintenance policies to contain the IPv6 security threats. They are also in need for understanding advantages and disadvantages of certain choices available for IPv6 physical and logical security. They are very familiar with vulnerabilities of IPv4 protocol since they have worked on them for a long time, but they are simply not quite as experienced with IPv6 vulnerabilities [6]. The malicious activities against the all-node link-local IPv6 multicast address (FF02::1) are attacks caused by security vulnerabilities that still need to be investigated and resolved. These attacks could be launched by sending ICMPv6 echo request packets, ICMPv6 packets with an invalid extension header, an MLD (Multicast Listener Discovery) query, or ICMPv6 Router Advertisement packet with a random address prefix [7]. The attacks against IPv6 tunnel transition mechanisms [8], duplicate address detection process [9], and IPv6 neighbor discovery protocol (NDP) [10] are dangerous attacks, still possible, and require in-depth studies and research to produce successful means of countering or at least mitigating them. On the other hand, criminals and hackers are very smart at exploiting available vulnerabilities and discovering new ones. They are constantly looking for new ways to hack and misuse any newly published technologies because these growing technologies can have major security issues and threats that the security community still ignore. Organizations around the world are increasingly finding themselves falling victim of hacking. The results of some recent studies showed that the rate of cyber-dependent crime and online fraud have increased significantly during the COVID-19 outbreak in the UK [11]. Therefore, it is crucial for investigators and researchers to understand the security issues that are related to IPv6 protocol and invent scientific and reliable solutions. The important questions that come to the minds of many professionals in the field are:

1. What is the volume of research published in IPv6 security?
2. Is there a significant global interest in research dedicated to IPv6 security issues?
3. What are the most important IPv6 security issues addressed in the research?

Researchers have published many ideas highlighting the security threats and the countermeasures, and to date, the prevalence rate of IPv6 deployment is still far from the desired rate despite the fact that more than 20 years have passed since the introduction of the IPv6 protocol [12]. The current study is a systematic literature review that follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology [13]. It aims to review the research of IPv6 in a systematic way. The main aspect of the study is to search the literature that allows us to understand the trends, attempts, and main arears in the field. In addition, the study maps the literature to realize the conclusions from the past 20 years and discuss the possible future scenario along with future agenda. There are several comprehensive survey papers on IPv6 security that have been published over the past decade [6, 8-9, 14-15], but based on our knowledge, this study is the first to address this topic using the systematic literature review and following PRISMA methodology [16].

The remainder of this paper is organized as follows: Section II explains the methodology of the study. The IPv6 security research analysis and classification results are reported in Section III. Section IV provides general interpretation of the results and summarizes the main findings. And finally, Section V concludes the research.

Methodology:

The PRISMA methodology is an easy to follow framework for reporting in systematic reviews and meta-analyses. It has been applied in many scientific fields such as autism spectrum disorder [17], biodiesel production [18], machine learning and deep learning [19], and student performance assessment [20]. Its framework could be summarized by four main stages: 1- developing search strategy, 2- applying selection criteria, 3- maintaining the quality of results, and 4- extracting the data. In the following sections these stages are described in detail.

Search Strategy

In order to perform the systematic search, a search strategy aiming at identifying the relevant literature is developed. This strategy is tailored to two databases: IEEE and Scopus. These two databases are among the most extensive databases of publications with powerful resources for accessing scientific and technical content. One search term used in querying the databases: “IPv6”. Based on the literature returned from the first search attempts, a decision to limit the search to the period 2000 – 2020 has been made.

Selection Criteria

The search conducted is mainly aiming at mapping existing literature on IPv6 protocol to the field of security. The search is narrowed to the Computer Science and Engineering science fields. The search span was for the last two decades, from year 2000, a few years after announcing the IPv6 technology, until year 2020. All studies that were not published in the period 2000 – 2020 were excluded. The search covered all countries of the world and no country was excluded, but the studies not published in English were excluded. Since the search criteria in IEEE and Scopus are slightly different in terms of criteria names and numbers, appropriate selection criteria were applied for each. In IEEE, the “publishing topic” criterion was set to "computer network security", which resulted in 4,185 studies out of 4,824 studies being excluded. Therefore, the total number of studies extracted from the IEEE is 639. Regarding the Scopus database, the “keyword” criterion was set to “network security”. The number of studies extracted is 517, while the total number extracted was 8,080 studies, meaning 7,563 studies were excluded. The final number of studies extracted from the two databases is 1156 studies. Table. 1, summarizes the selection criteria step.

Table 1. Selection criteria step

	IEEE	Scopus
Keyword:	“IPv6”	“IPv6”
criterion applied:	“publishing topic”	“keyword”
value of criterion:	"computer network security"	“network security”
records returned:	4824	8080
records excluded:	4185	7563
records extracted:	639	517

Maintaining Quality

For maintaining the quality of the review, three main tasks have been carried out over the results of the search:

1. Filter based on article type: this task is carried out by filtering the “document identifier” field in the IEEE database and the “document type” field in the Scopus database. All studies that are not research papers, review papers, or conference papers have been excluded from the studies list. The studies published in IEEE magazines are excluded as these studies might be tutorials or summaries updating a technical area. As a result, 25 studies were excluded from IEEE database and 2 studies were excluded from Scopus database.
2. Exclusion of duplicated studies: this task is simply implemented by making use of the features available in the MS Excel, i.e. removing duplicate in the data tab and using the match function. It was carried out in two stages:
   2.1 Examining studies in each database separately for duplicates: this resulted in excluding 9 studies from the IEEE database and 3 studies from the Scopus database.
   2.2 Examining studies in the two databases together for duplicates: this resulted in excluding 92 studies from the Scopus database.
3. Evaluation of studies: this task took place in two stages:
   3.1 Each study was carefully evaluated by reading and analysing the abstract to select only studies that investigate IPv6 network security. Not all studies were equally relevant for inclusion in the list. For example, studies that looked at IoT only or looked at 3g and/or 4g networks were excluded. Therefore, 193 studies were excluded from the IEEE database and 148 studies were excluded from the Scopus database.
   3.2 The studies that were not cited and published five or more years ago, i.e. number of article citations = 0 and year of publication <= 2015, were excluded. These studies were excluded as the lack of citations after five years of publishing a research reflects a weakness in the research contribution. As a result, 168 studies were excluded from IEEE database and 89 studies were excluded from Scopus database.

Table 2 displays statistics of studies after implementing the tasks of the maintaining quality stage.

Table 2. Maintaining quality stage

Task	Step	Excluded studies	
		IEEE	Scopus
Filter based on article type	Including research, review, and conference papers	25	2
Exclusion of duplicated studies	Excluding duplicates in the one database	9	3
	Excluding duplicates in the two databases	0	92
Evaluation of studies	Reading and analyzing the abstract	193	148
	Excluding uncited studies	168	89
Total of Remaining studies:		244	183

Extracting the Data

In the data extraction phase, a total of 427 studies were selected from the two databases. Data extracted from the selected studies involved: authors, title, year, volume, issue, page count, affiliations, authors with affiliations, abstract, author keywords, funding details, reference count, article citation count, and document type. Fig. 1, shows the flow chart of inclusion and exclusion process according to the PRISMA guidelines.

Data Analysis

The aim of the data analysis task was to identify clues relating to the review's objectives and questions. Three different classification processes have been performed. The title, abstract and keywords were the basic data adopted during the analysis process as they were analyzed meticulously. First, each study was classified as either "conceptual contribution" or "practical contribution". The "conceptual contribution" class means that the research described, analyzed, compared, or reviewed a research topic, and the "practical contribution" class means that the research proposed, presented, designed, or developed a system or program to solve an existing problem after presenting it in detail. Another classification was performed which was according to the scope of the study. Scope refers to the extent to which an IPv6 research area is explored and the parameters within which the study will be operating. For example, a researcher wanted to study how to secure an IPv6 communication type in wireless networks and he covered the multicast type communication along with the MLD 2 (Multicast Listener Discovery) component in his study, so the classification of his study will be represented by the string of "wireless network; IPv6: multicast; MLD2". This string has two sides separated by colon, right side or the field(s) and left side or the parameter(s). The left side represents the scope that the researcher worked on and the right side represents the parameters that the researcher dealt with. The components of either sides are separated by semicolons. The third classification made is the classification of studies according the problem they aim to solve. For example, "DoS Detection", "Packet Classification", etc.

Results:

This section reports the results of applying PRISMA methodology based upon the data gathered. To report the results in an orderly manner following a logical sequence, this section is divided into two parts, descriptive analysis and the literature classification [21].

Descriptive Analysis

A- The annual number of publications and citations:

Figs. 2 and 3, show the number of studies published and the total number of citations in the years 2000 – 2020 for IEEE and Scopus databases. The number of studies published in IEEE and Scopus during the decade 2000 – 2010 was 97 and 50 studies, respectively. While the number of publications during the second decade 2011 – 2020 reached to 147 and 183 studies. The number of citations has also increased rapidly. The total of citations for IEEE and Scopus publications during the first decade 2000 – 2010 was 409 citations, and increased significantly during the second decade 2011 – 2020, reaching 1643 citations.

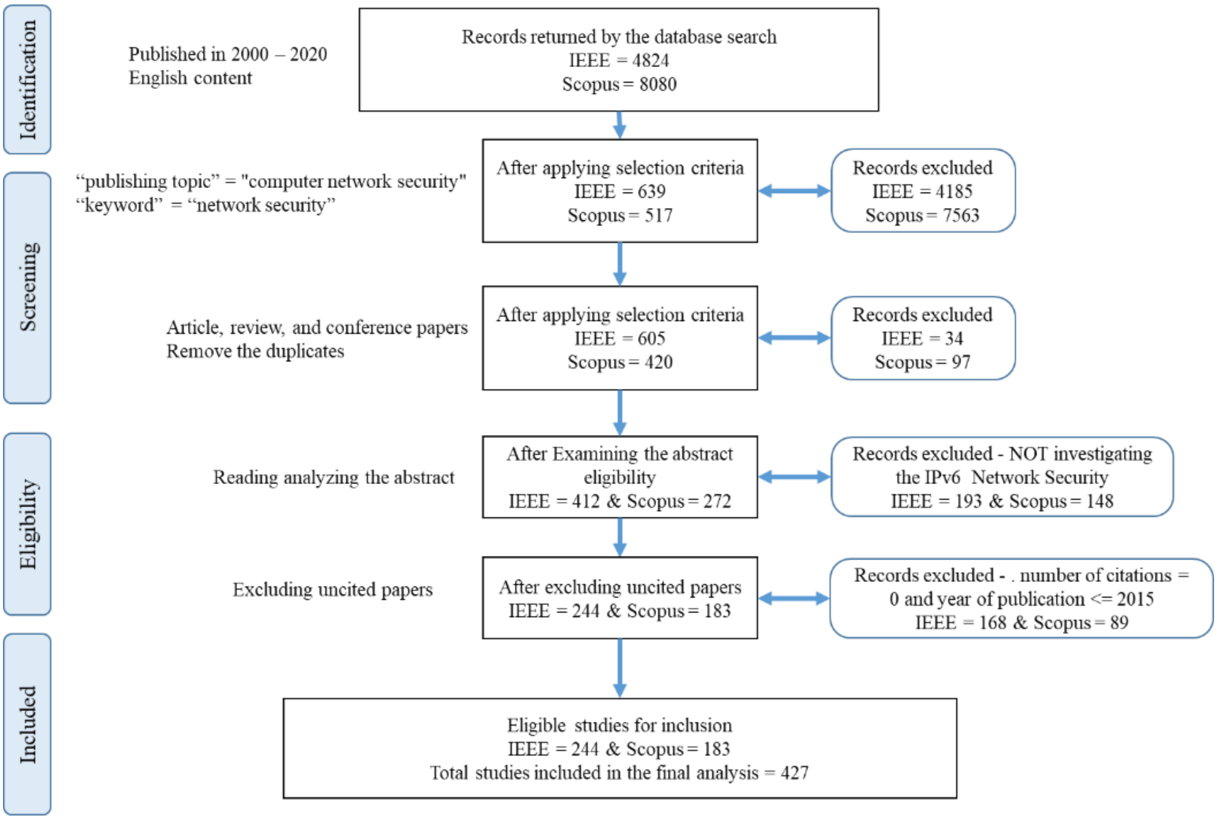
Identification
Published in 2000 – 2020
English content
Records returned by the database search
IEEE = 4824
Scopus = 8080
Screening
"publishing topic" = "computer network security"
"keyword" = "network security"
After applying selection criteria
IEEE = 639
Scopus = 517
Records excluded
IEEE = 4185
Scopus = 7563
Article, review, and conference papers
Remove the duplicates
After applying selection criteria
IEEE = 605
Scopus = 420
Records excluded
IEEE = 34
Scopus = 97
Eligibility
Reading analyzing the abstract
After Examining the abstract eligibility
IEEE = 412 & Scopus = 272
Records excluded - NOT investigating the IPv6 Network Security
IEEE = 193 & Scopus = 148
Excluding uncited papers
After excluding uncited papers
IEEE = 244 & Scopus = 183
Records excluded - . number of citations = 0 and year of publication <= 2015
IEEE = 168 & Scopus = 89
Included
Eligible studies for inclusion
IEEE = 244 & Scopus = 183
Total studies included in the final analysis = 427

Figure 1. Flow diagram of study selection.

B- The percentage of publications by type:

Figs. 4 and 5, illustrate the percentages of studies according to the types. The largest percentage 89.75% of IEEE publications was for the conference type, while percentages of journal research and review papers were 8.20% and 2.05% respectively. Regarding the Scopus publications, the largest percentage of publications was also of the conference type, which is 63.39%, but the percentage of journal papers published is 34.43%, greater than that of the IEEE. The percentage of review papers was the lowest in both databases, it was 2.05% in IEEE and 2.19% in Scopus.

C- The percentage of publications by region:

The percentages of studies were calculated for IEEE and Scopus databases according to the regions of the world as in Figs. 6, 7. The aim of these calculations is to shed more light on the active regions in IPv6 security research. The regions were extracted either by knowing the country to which the main author belongs, or by the country name mentioned in the title or in the abstract. It is clear that the largest percentages of studies published in IEEE (59.43%) and Scopus (60.11%) come from Asia, then Europe comes second and North America comes third in both databases.

D- Percentage of funded research:

Since the funded research can enhance the IPv6 security research and reflects an institutional interest in the field, the percentage of funded research and the percentage of unfunded research were calculated as in Figs. 8 and 9. The rates of funded research published in both IEEE and Scopus are 5.74% and 16.39%, respectively.

Literature Classification

A- Classification of studies based on the type of contribution:

Fig. 10 displays the number of studies that have been classified into "practical contribution" and the number of studies that have been classified into "conceptual contribution" for each database. The large number of studies published in both databases were classified as "practical contribution", 175 in IEEE and 141 in Scopus. This means more 70% of the research published in IEEE and Scopus aimed at providing a practical solution to a security problem in the IPv6 protocol.

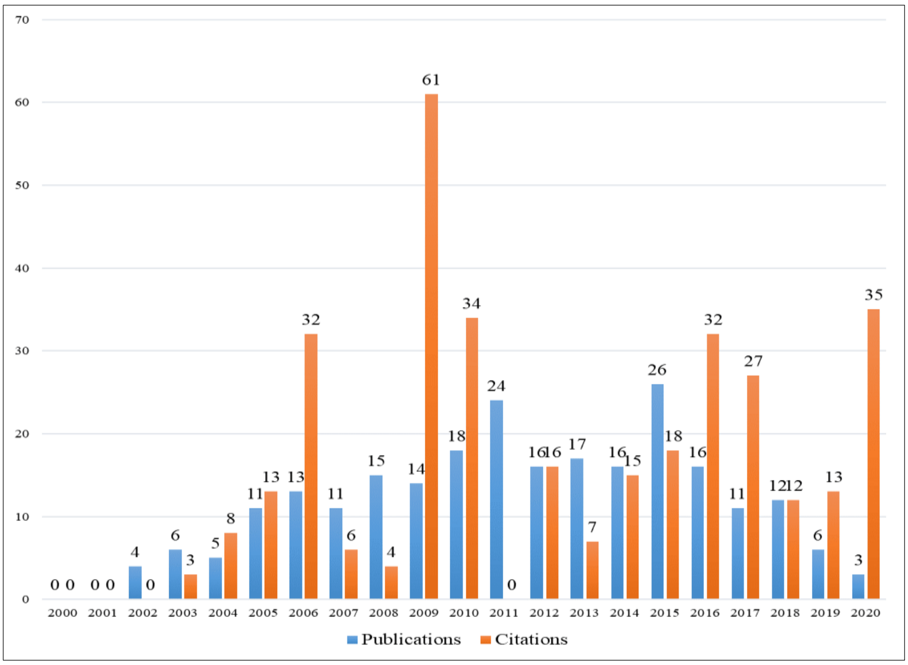

Figure 2. Number of publications and citations per year for IEEE database

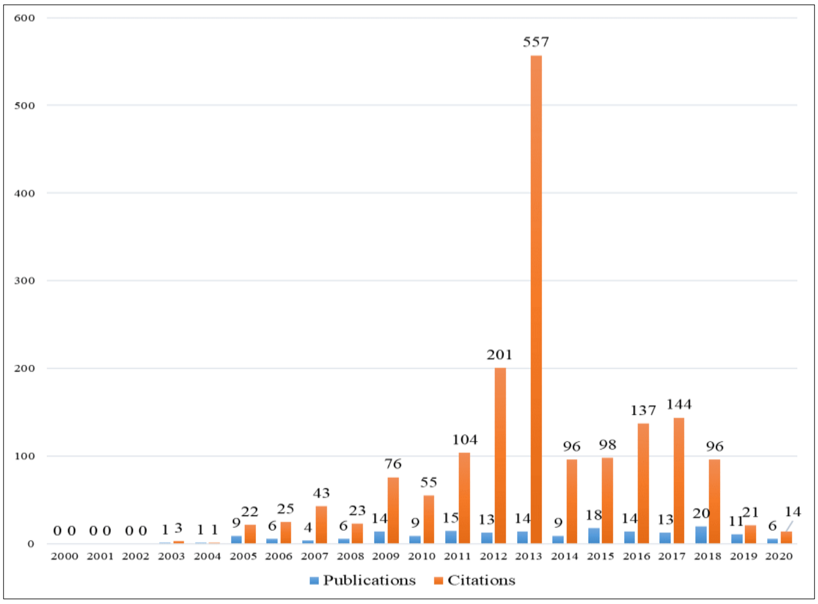

Figure 3. Number of publications and citations per year for Scopus database

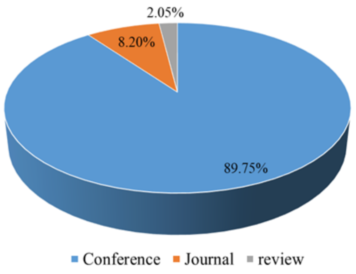

Figure 4. Percentage of studies according to the types for IEEE database

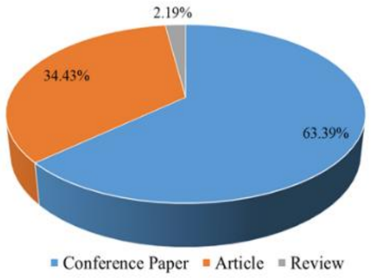

Figure 5. Percentage of studies according to the types for Scopus database

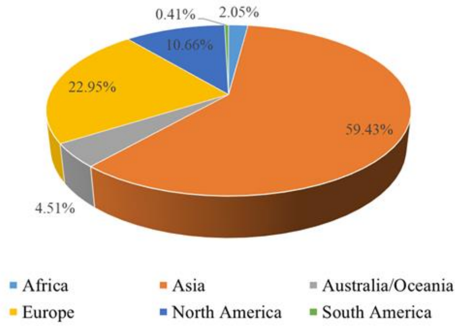

Figure 6. Percentage of IEEE studies according to the region

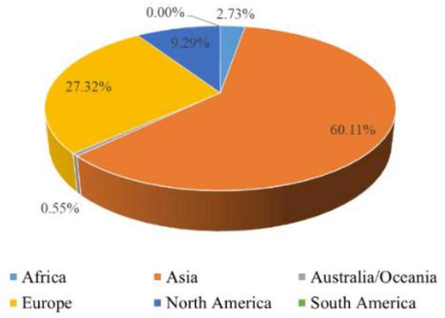

Figure 7. Percentage of Scopus studies according to the region

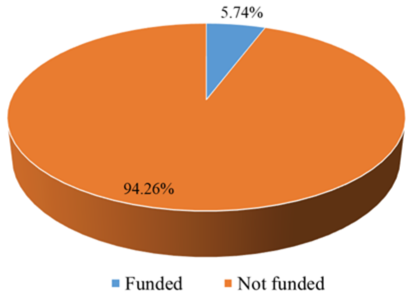

Figure 8. Percentage of funded research published in IEEE

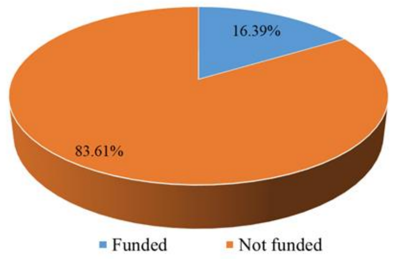

Figure 9. Percentage of funded research published in Scopus

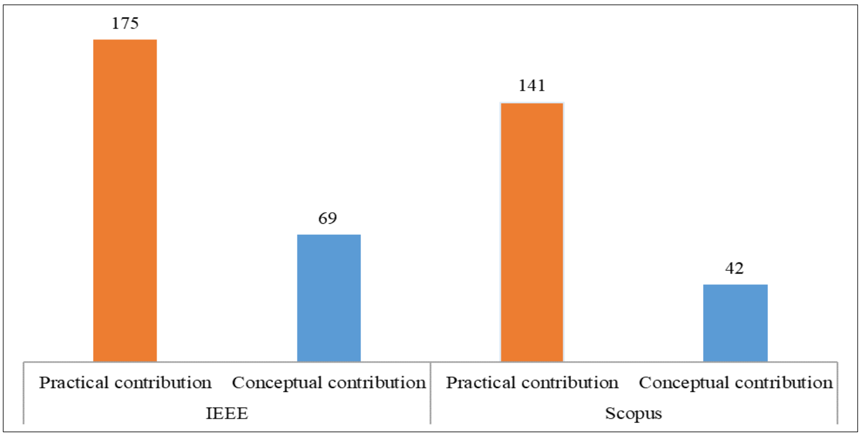

Figure 10. Classification of studies based on the type of contribution

B- Classification of studies based on the scope and problem:

Table. 3, presents the results of categorizing studies according to the scopes in order to find out more about the research areas related to the IPv6 protocol that were addressed. The first column represents the category, and it is the left side of the scope string. Since the number of parameters is large in some fields, they are not displayed, rather their numbers are displayed for each category as in the second column. The third column shows the database. As for the fourth and fifth columns, they indicate the number of studies and their percentage to the studies published in the database and categorized for the category mentioned in the first column. The “IPv6” category contained the largest percentage of studies published in the two databases, 41.80% for IEEE and 42.08% for Scopus. The studies classified in this category addressed 64 parameters in IEEE and 95 parameters in Scopus, examples of parameters include: DHCPv6, ICMPv6, NDP, SeND, SLAAC, DAD, IPsec, AAA protocol, CGA, cryptographic hash function, BGP routing tables, NAT64, DNS64, DNSv6, IP trackback, IPv6 flows, and IPv6 packets. The studies attempted to address and solve many research problems, for examples: enhancing the anonymity of the host [22], Router Advertisement flooding attacks detection [23], IPv6 traffic monitoring [24], MITM attack detection [25], and DoS detection [26]. Most of these studies were of the practical contribution type. The relationship between the IPv4 and IPv6 protocols has been significantly examined in the literature. The studies considered in this paper that addressed these two protocols together are grouped into a category called “IPv4; IPv6”. The percentage of studies in this category was 13.93% in IEEE and 8.74% in Scopus. The largest percentage of studies have addressed the challenges of moving to IPv6, with 16 of the 34 studies published in IEEE and 11 of the 16 studies published in Scopus. Most of these studies were of the type of practical contributions that proposed solutions to security issues of IPv6 transition methods such as securing IPv6 transition [27-29] and dual stack issues [30-31]. However, some studies of the conceptual contribution type have provided a comprehensive survey of IPv6 transition methods with a focus on security [32]. There are also other studies that examining the detection of special attacks in dual stack networks such as spoofing [33], ICMPv6 DoS flooding [34], and anomaly behaviors [35]. The “IoT” category also attracted the attention of researchers. The percentages of studies in this category were 9.43% and 13.66% for IEEE and Scopus respectively, with a remarkable percentage of studies from conceptual contribution type. Research in this category has mainly focused on two parameters, 6LoWPAN protection and encryption methods. Examples of the research problems that have been tackled include node misbehavior detection [36], identification of securing 6LoWPAN techniques [37], and securing group handover [38]. Some studies have focused on the routing protocol for wireless networks, the RPL protocol to address some issues in IPv6 security over IoT such as detecting excessive broadcasts [39], Blackhole attacks detection [40], detection Sybil attack [41-42], 6LoWPAN security of link-layer protocol headers[43], and DNSv6 authentication. The research areas MIPv6 and PMIPv6 formed two distinct classes. Since the only bulk difference between the two fields is that the MIPv6 is a host-based protocol, while PMIPv6 is a network-based protocol [44], they were treated as one category. Total studies in this category were 44 studies, and the percentage of parameters that are related to IPv6 security was 66%. Examples of these parameters are CPK-based authentication, AAA protocol, IPSec, binding update, and twofold encryption. Several IPv6 security issues addressed by the studies in this category, examples include securing the network access and data transmission [45], enhancing the authentication process during mobile nodes hand off [46], securing binding updates [47], and intrusion detection in mobile IPv6 networks [48]. Some studies have focused on parameters related to the operations of MIPv6 and PMIPv6 such as nodes location update, binding update, route optimization, and Mobile Node and Correspondent Node hand over schemes. However, the objectives of the studies were not far from the topic of IPv6 security, examples of objectives include solving inadequacy of the protection of proxy update and acknowledgement messages [49], detecting MITM, hijacking, and DoS attacks [50-51], and detecting unauthenticated and unauthorized binding update attacks [52]. Table 4 provides examples of studies from some other categories with explanation of the parameters that the studies worked on and the issues that they tried to solve.

Table 3. Classification of studies based on scopes

Category: field(s)	No of parameters	Database	Count	Rate
ad hoc networks;IPv6	1	IEEE	1	0.41%
Cloud computing;IPv6	1	IEEE	1	0.41%
FMIPv6	4	Scopus	2	1.09%
heterogeneous networks;MIPv6	2	Scopus	1	0.55%
Heterogeneous Wireless;IPv6	1	IEEE	1	0.41%
IoT	10	IEEE	23	9.43%
	23	Scopus	25	13.66%
IoT;IPv6	7	IEEE	8	3.28%
	11	Scopus	8	4.37%
IoT;M2M	2	Scopus	1	0.55%
IPv4;IPv6	20	IEEE	34	13.93%
	14	Scopus	16	8.74%
IPv4;IPv6;P2P	1	IEEE	1	0.41%
IPv6	64	IEEE	102	41.80%
	95	Scopus	77	42.08%
IPv6;Tunnel protocols	1	IEEE	1	0.41%
IPv6;VM	2	Scopus	1	0.55%
ITS;IPv6	2	Scopus	1	0.55%
LAN;IPv4;IPv6	2	IEEE	1	0.41%
LAN;IPv6	2	IEEE	2	0.82%
	9	Scopus	4	2.19%
LAN;Local Link;IPv6	1	Scopus	1	0.55%
M2M	1	IEEE	1	0.41%
	2	Scopus	1	0.55%
MANET;IPv6	3	IEEE	2	0.82%
	4	Scopus	2	1.09%
MIPv6	14	IEEE	13	5.33%
	33	Scopus	23	12.57%
MIPv6;IPv6	3	Scopus	1	0.55%
NEMO	5	IEEE	5	2.05%
NEMO;FMIPv6	1	IEEE	1	0.41%
NEMO;MIPv6	15	IEEE	16	6.56%
	1	Scopus	1	0.55%
NEMO;PMIPv6	3	IEEE	5	2.05%
NEMO;VANET	1	IEEE	1	0.41%
P2P;IPv6	1	Scopus	1	0.55%
PMIPv6	3	IEEE	2	0.82%
	8	Scopus	5	2.73%
SDN;IPv6	1	IEEE	1	0.41%
	2	Scopus	1	0.55%
SH-IoT;PMIPv6	1	IEEE	1	0.41%
VANET;IPv6	2	Scopus	1	0.55%
Wireless;IPv4;IPv6	1	IEEE	1	0.41%
	1	Scopus	1	0.55%
Wireless;IPv6	5	IEEE	4	1.64%
WLAN;IPv6	2	IEEE	2	0.82%
WSN	5	IEEE	7	2.87%
	3	Scopus	3	1.64%
WSN;6LoWPAN	1	IEEE	1	0.41%
WSN;IPv6	4	IEEE	6	2.46%
	8	Scopus	5	2.73%
WSN;IPv6-based WSN	2	Scopus	1	0.55%

Table 4. Examples of studies of selected categories

Category: field(s)	Examples of parameters	Type	problem/purpose	DB	Reference
Cloud computing;IPv6	Economic Denial of Sustainability (EDoS)	conceptual contribution	Reviewing various EDoS mitigation techniques	IEEE	53
IoT;M2M;IPv6	6LoWPAN; Authentication	practical contribution	DoS attack detection	IEEE	54
IPv4;IPv6;P2P	WPA2; scanning worms	conceptual contribution	Evaluating the effect of WPA2 security 802.11n bandwidth wireless P2P for both IPv4 and IPv6	IEEE	55
		conceptual contribution	Modelling and analyzing spread of two-phase scanning in IPv6	Scopus	56
IPv6;Learning	Learning IPv6	practical contribution	Lack of IPv6 learning kit	IEEE	57
LAN;IPv4;IPv6	advanced routing and scanning worms	practical contribution	Routing worms and scanning worms detection	IEEE	58
LAN;Local Link;IPv6	NDP; host identity;IPv6 address assignments	practical contribution	RA flood attack detection	IEEE	59
		practical contribution	host identity detection in IPv6 networks	Scopus	60
SDN;IPv6	NDP;SLAAC; IP packets	practical contribution	Traceback and identification of attackers in IPv6 networks	IEEE	61
		practical contribution	Securing the IPv6 (NDP) message exchange and make the SLAAC safer	Scopus	62
Wireless;IPv4;IPv6	IPSec; encryption ;key management	practical contribution	Creating IPv6 attack testbed	IEEE	63
		practical contribution	Filtering illegal accesses to wireless IPv6 networks	IEEE	64
WSN;6LoWPAN	PKI; NDP;RPL, Neuro-fuzzy;DoS	practical contribution	Integrating 6LoWPAN with PKI	IEEE	65
		practical contribution	Preventing unauthorized nodes from using the network	IEEE	66
		practical contribution	Lowering the mobility handover cost and packet loss rate	Scopus	67
		practical contribution	Intrusion detection in RPL-connected 6LoWPAN	Scopus	68
		practical contribution	classifying the IPv6 packets to detect Router Alert Option DoS Packets	Scopus	69

Discussion:

An evidence from the literature on IPv6 security is presented in this systematic review. From two public databases, IEEE and Scopus, a total of 12,904 studies published during the period 2000 – 2020 were examined. Only the 427 studies that helped spread knowledge about IPv6 vulnerabilities and how to address them were selected. Among the published studies on the IPv6 protocol, a significant number of studies have explored security issues, and they were often devoted to discussing IPv6 security issues Ethernet, wireless, and mobile networks. There is a number of studies that explored security issues in the operational protocols such as ICMPv6 and in the transition methods from IPv4 to IPv6 such as dual stack, tunnels, and NAT64/DNS64. There were a number of studies devoted to exploring methods of mitigating or detecting malware attacks, and all of these studies were worth taking into consideration. Consequently, a filtering process was carried out in three stages to include only the studies that serve the purpose of the review, and these stages were: filtering based on article type (research, review, and conference papers), exclusion of duplicated studies, and evaluation of studies (abstract, keyword, and title).

Recent reviews of IPv6 security issues have focused on existing attacks in IPv6, IPSec, common threats in both IPv4 and IPv6, and security issues related to transition methods, and thus also been able to provide relatively straightforward conclusions or recommendations. Based on their review of malicious attacks in IPv6, A. Shiranzaei and R. Z. Khan [70], for example, concluded that IPv6 raises new security challenges despite the new security functionalities and despite the fact that IPSec is mandatory to setup in the new protocol. In fact, this is similar to the conclusion of this review. However, expanding the review to include studies addressing IPv6 security issues in a specific environment, such as the IoT, wireless, and local link will lead to further conclusions. In their systematic review of FMIPv6 enhancements, some researchers concluded that the unique operational features of FMIPv6 can potentially address some of very complex mobility management challenges in IPv6-based 5G network [71]. Since this review has a more general focus, such conclusion could not be reached. The analysis and classification of the literature followed in this review raised several important insights and allowed some recommendations for further research. The first key finding shows that there is a significant increase in the IPv6 security literature after 2005. In the sense that interest in this field of research began more than 15 years ago, meaning that this field of research is relatively still in its infancy to some extent. In contrast with the first decade, the second decade has witnessed an obvious increase in the research publications. The number of researches published in the first decade 2000 – 2010 was 147 while it increased to 330 in the second decade 2011 – 2020, meaning that the percentage of increase was 124%. The number of citations is another factor might reflect a significant global interest in research dedicated to IPv6 security issues. It was 409 in the first decade, then it increased to 1643 citations during the second decade, meaning that the percentage of increase was 302%. However, the largest percentage of published research, which is about 78%, was of the conference type. Generally, in most fields, the research studies published in well-known journals tend to have a greater rank than the research studies presented in famous conferences or published in their proceeding. Consequently, more studies regarded as very high quality work, i.e. published in well-known journals, would be needed to fill this gap.

The largest percentage of studies, which was 60% comes from Asia, and the percentage of studies funded by countries of the Asian continent to the percentage of studies funded by countries of other continents was 64%. It can be concluded from these two percentages that the countries of Asia are more involved in researching security issues for IPv6 than other countries of the world. However, this does not necessarily mean that the countries of Asia have the highest percentage in terms of IPv6 deployment. According to some recent analytics, the top five countries with highest estimated number of IPv6 users worldwide contain three countries from Asia along with USA and Brazil as well [72]. The scope of IPv6 was explored in a high percentage of the studies that were reviewed, exceeding 40%. Various vulnerabilities, exploitation and attacks were also addressed. Mitigation and detection methods were suggested in operational and regulatory protocols in IPv6 technology such as NDP, IPSec, DHCPv6, NAT64, DNS64, DNSv6, and ICMPv6. This is the main reason why the percentage of studies aimed at providing a practical solution to a security issue was more than 70% in both databases. This finding can bring very positive connotations to mind, since such kind of studies are an increasingly important component of proactively assessing flaws in the fabric of IPv6 technology and fixing them, and thus securing the new protocol against malicious attacks. However, there is a necessary need for more studies with conceptual contributions to clarify the state of knowledge, explain apparent flows, and identify needed research within the scope of IPv6 protocol. A total of 50 studies addressed both IPv4 and IPv6 and more that 50% of these studies examined the security challenges of IPv6 transition. There were distinct efforts exerted to present challenges and methods to overcome them, and the percentages of conceptual contributions and practical contributions were 40% and 60% respectively. However, by comparing these studies, it was found that the least effort was for dual stack and NAT64. These two transition methods are currently the preferred ones, as the general trend for migration is either to dual stack or to native IPv6 [73]. Given the importance and effectiveness of these two transition methods, this may be an important area to explore further with regard to security challenges.

Researching IPv6 security issues in IoT, WSN, and MIPv6 environments has drawn much attention. This research began to appear since 2011, a period that also witnessed the beginning of interest in the IoT and WSN technologies. The percentage of studies reviewed in this paper that examined these scopes was 40.52%, most of which, around 79.19%, was devoted to solving security issues related to the IPv6 protocol, and most of these issues was about the authentication, encryption, and detection of famous attacks. It was, however, in relation to the traffic monitoring, that the gaps in the literature were most evident. Even though a few papers explored IPv6 traffic monitoring in IoT, WSN, and MIPv6, traffic classification and packet inspection topics were significantly under researched areas. The studies reviewed in this paper were from IEEE and Scopus databases. It thus has to be acknowledged, that the studies may represent a particular set of IPv6 scopes, parameters, and research problems. No major differences in terms of scopes, parameters, and research problems were identified in the studies included from IEEE and from Scopus. To make any firm comparison, more literature from other databases would be required. Finally, the utilization of ICMPv6 vulnerabilities and DNSv6 and DHCPv6 services vulnerabilities in Ethernet and wireless networks are areas which would benefit from being researched in further depth. Moreover, they could be expected to contribute positively and significantly to the migration from IPv4 to IPv6.

Conclusion:

This systematic review has analyzed the literature on the next Internet protocol technology, the IPv6 with a focus on security issues. A topic which is rarely explored from a qualitative perspective. The review concluded to a number of key findings that shows positive signs of published research and contributions in the field. For example, there is a significant increase in the IPv6 security literature after 2005 and also the scope of IPv6 was explored in a high percentage. Additionally, a lot of important parameters have been examined in terms of the IPv6 security such as NDP, SeND, DAD, SLAAC, IPSec, and 6LoWPAN. However, a number of important gaps were also identified. To fully understand the vulnerabilities that may hinder the deployment of IPv6, more comprehensive studies, which explicitly clarify the state of knowledge, explain apparent flows, and identify needed research within the scope of IPv6 protocol. Moreover, any effort devoted to explore the dual stack and NAT66, which are the general trend for migration to IPv6 would be a welcome addition. Finally, the IPv6 traffic classification and packet inspection topics need to be extended to cover the IoT, WSN, and MIPv6 environments rather than limited these topics on the Ethernet and local link networks.

Authors' declaration:

- Conflicts of Interest: None.
- The authors hereby affirm that all figures and tables in the manuscript are their own.
- Ethical Clearance: The project was approved by the local ethical committee in Sultan Qaboos University.

Authors' contributions statement:

S. A. Conceptualization and Design, Literature Review, and Methodology. A. A. Investigation and Data Collection, Data Analysis and Interpretation, and proofreading. All authors reviewed the results and approved the final version of the manuscript

References

1. Cui Y, Wu P, Xu M, Wu J, Lee YL, Durand A, et al. 4over6: network layer virtualization for IPv4-IPv6 coexistence. IEEE Network. 2012; 26(5): 44-8.
2. Javaid N, Sher A, Nasir H, Guizani N. Intelligence in IoT-based 5G networks: Opportunities and challenges. IEEE Commun. Mag. 2018; 56(10): 94-100.
3. Abdulzahra SA, Al-Qurabat AK, Idrees AK. “Compression-based Data Reduction Technique for IoT Sensor Networks”, Baghdad Sci J. 2021; 18(1): 1840198
4. Davies J. Understanding IPv6: Understanding IPv6 _p3: Pearson Education; 2012. Available from: https://www.amazon.com/Understanding-IPv6-_p3-ebook/dp/B00JDMPHT0
5. Google.com. IPv6 Capable Rate by country [Internet]. 2022 [update 2022 July 1; cited 2022 July 1]. Available from: https://stats.labs.apnic.net/ipv6.
6. Lencse G, Kadobayashi Y. Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis. IEICE Trans Commun. 2019; 102(10): 2021-35.
7. Khan AA, Ali SA. Network forensics investigation: Behaviour analysis of distinct operating systems to detect and identify the host in IPv6 network. Int J Electron Secur Digit Forensics. 2021;1 3(6): 600-11.
8. Abdulla SA. Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms. Int J Netw Secur. 2017; 12(2): 83-102.
9. Al-Ani AK, Anbar M, Manickam S, Wey CY, Leau Y-B, Al-Ani A. Detection and defense mechanisms on duplicate address detection process in IPv6 link-local network: A survey on limitations and requirements. Arab J Sci Eng. 2019; 44(4): 3745-63.
10. Anbar M, Abdullah R, Saad R, Alomari E, Alsaleem S. Review of security vulnerabilities in the IPv6 neighbor discovery protocol. Inform Sci-Appl.(ICISA). 2016 : 603-612. Springer, Singapore.
11. Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. Eur Soc. 2021 Feb 19; 23(sup1): S47-59.
12. Dawadi BR, Rawat DB, Joshi SR, Manzoni P, Keitsch MM. Migration cost optimization for service provider legacy network migration to software-defined IPv6 network. Int J Netw Manag. 2020: e2145.
13. Moher D, Liberati A, Tetzlaff J, Altman DG. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Int J Surg. 2010; 8(5): 336-41.
14. Supriyanto, Hasbullah IH, Murugesan RK, Ramadass S. Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods. IETE Tech Rev. 2013; 30(1): 64-71.
15. Modares H, Moravejosharieh A, Lloret J, Salleh R. A survey of secure protocols in mobile IPv6. J Netw Comput Appl. 2014; 39: 351-68.
16. Lencse G, Kadobayashi Y. Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of

DNS64 and stateful NAT64. Comput Secur. 2018 Aug 1; 77: 397-411.

17. Allely CS. Understanding and recognising the female phenotype of autism spectrum disorder and the 'camouflage'hypothesis: A systematic PRISMA review. Adv Autism. 2019; 5 (1): 14–37.
18. Ortiz-Martínez VM, Andreo-Martinez P, Garcia-Martinez N, de los Ríos AP, Hernández-Fernández FJ, Quesada-Medina J. Approach to biodiesel production from microalgae under supercritical conditions by the PRISMA method. Fuel Process Technol. 2019; 191: 211-22.
19. Nosratabadi S, Mosavi A, Duan P, Ghamisi P, Filip F, Band SS, et al. Data science in economics: comprehensive review of advanced machine learning and deep learning methods. Mathematics. 2020; 8(10): 1799.
20. Amelia N, Abdullah AG, Mulyadi Y. Meta-analysis of student performance assessment using fuzzy logic. Indones J Sci Technol. 2019; 4(1): 74-88.
21. Gravetter FJ, Wallnau LB, Forzano L-AB, Witnauer JE. Essentials of statistics for the behavioral sciences: Cengage Learning; 2020.
22. Gao T, Deng X, Guo N, Wang X. An anonymous authentication scheme based on PMIPv6 for VANETs. IEEE Access. 2018 Feb 28; 6: 14686-98.
23. Anbar M, Abdullah R, Al-Tamimi BN, Hussain A. A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks. Cognit Comput. 2018; 10(2): 201-14.
24. Beck F, Chrisment I. A monitoring approach for safe IPv6 renumbering. Int Multiconf Comp Glob. Inf Technol. (ICCGI'06) 2006 Aug 1 : 1-6. IEEE.
25. Shah JL. A novel approach for securing IPv6 link local communication. Inf Secur J. 2016; 25(1-3): 136-50.
26. Wang Y, Tong S, Yang Y. A practical hybrid IP traceback method under IPv6. J Converg Inf Technol. 2012; 7: 173-82.
27. Li KH, Wong KY. Empirical analysis of IPv4 and IPv6 networks through dual-stack sites. Information. 2021 Jun 14; 12(6): 246.
28. Boukerche A, Zhang Q. Countermeasures against worm spreading: A new challenge for vehicular networks. ACM Comput. Surv. 2019 May 30; 52(2): 1-25.
29. Malik M, Dutta M. Implement ation of single-packet hybrid IP traceback for IPv4 and IPv6 networks. IET Inf Secur. 2017; 12(1): 1-6.
30. Kao YC, Liu JC, Ke YQ, Tsai SC, Lin YB. Dual-stack network management through one-time authentication mechanism. IEEE Access. 2020 Feb 18; 8: 34706-16.
31. Dawadi BR, Rawat DB, Joshi SR. Software defined ipv6 network: A new paradigm for future networking. JIE. 2019 Jul 31; 15(2): 1-3.
32. El Khadiri K, Labouidya O, Elkamoun N, Hilal R. Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET modeler. Int J Adv Comput Sci Appl. 2018; 9(4): 387-392.
33. Tian DJ, Butler KR, Choi JI, McDaniel P, Krishnaswamy P. Securing ARP/NDP from the ground up. EEE Trans Inf Forensics Secur. 2017; 12(9): 2131-43.
34. Singh R, Ranga V. Performance evaluation of machine learning classifiers on Internet of Things security dataset. Int J Control Autom. 2018 May; 11(5): 11-24.
35. Anbar M, Abdullah R, Al-Tamimi BN, Hussain A. A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks. Cognit Comput. 2018; 10(2): 201-14.
36. Kamaleshwar T, Lakshminarayanan R, Teekaraman Y, Kuppusamy R, Radhakrishnan A. Self-Adaptive Framework for Rectification and Detection of Black Hole and Wormhole Attacks in 6LoWPAN. Wirel. Commun Mob Comput. 2021; 2021: 1-8.
37. Verma A, Ranga V. Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT. Wirel Pers Commun. 2019 Oct; 108(3): 1571-94.
38. Qiu Y, Ma M. Secure group mobility support for 6lowpan networks. IEEE Internet Things J. 2018; 5(2): 1131-41.
39. Qureshi KN, Rana SS, Ahmed A, Jeon G. A novel and secure attacks detection framework for smart cities industrial internet of things. Sustain Cities Soc. 2020 Oct 1;61:102343.
40. Simoglou G, Violettas G, Petridou S, Mamatas L. Intrusion detection systems for RPL security: a comparative analysis. Comput Secur. 2021;104:102219.
41. Bang AO, Rao UP. A novel decentralized security architecture against sybil attack in RPL-based IoT networks: a focus on smart home use case. J Supercomput. 2021 Dec;77(12):13703-38.
42. Pu C. Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses. IEEE Internet Things J. 2020;7(6):4937-49.
43. Miguel ML, Jamhour E, Pellenz ME, Penna MC. SDN architecture for 6LoWPAN wireless sensor networks. Sensors. 2018 Nov 2; 18(11): 3738.
44. Yan Z, Zhou H, Wang H-C, Zhang H, Zhang S. Design and implementation of a hybrid MIPv6/PMIPv6-based mobility management architecture. Math Comput Model. 2011; 53(3-4): 421-42.
45. Shah JL, Bhat HF, Khan AI. CloudIoT: towards seamless and secure integration of cloud computing with Internet of Things. IJDCF. 2019 Jul 1; 11(3): 1-22.
46. Leiter Á, Bokor L. A flow-based and operator-centric dynamic mobility management scheme for proxy mobile IPv6. Wirel Commun Mob Comput. 2019; 2019: 1-21
47. Mathi S. An optimize d and secure BUTE–binding update using twofold encryption for next generation IP mobility. J Intell Fuzzy Syst. 2018; 34(3): 1311-22.
48. Tajdini M. Developing an Advanced IPv6 Evasion Attack Detection Framework. [PhD dissertation]. Liverpool John Moores University (UK); 2018. Available from: https://researchonline.ljmu.ac.uk/9864/1/2018TajdiniPhD.pdf
49. Mathi S, Khatri A, Sethuraman M, Anbarasi P. A secure and optimized location update for next

generation proxy mobility based internet protocol networks. J. Intell. Fuzzy Syst. 2019; 36(3): 2443-53.

50. Samir NM, Musni M, Hanapi ZM, Radzuan MR. Impact of Denial-of-Service Attack on Directional Compact Geographic Forwarding Routing Protocol in Wireless Sensor Networks. Baghdad Sci J. 2021 Dec 20; 18(4): 1371-7
51. Modares H, Mora. A, Salleh RB, Lloret J. Enhancing security in mobile IPv6. ETRI J. 2014; 36(1): 51-61.
52. Mathi SE, Valarmathi M. An enhanced binding update scheme for next generation internet protocol mobility. J Eng Sci Technol. 2018 Mar 1; 13(3): 573-88.
53. Shawahna A, Abu-Amara M, Mahmoud AS, Osais Y. EDoS-ADS: an enhanced mitigation technique against economic denial of sustainability (EDoS) attacks. IEEE Trans Cloud Comput. 2018 Feb 14; 8(3): 790-804.
54. Al-Kaseem BR, Al-Dunainawi Y, Al-Raweshidy HS. End-to-end delay enhancement in 6LoWPAN testbed using programmable network concepts. IEEE Internet Things J. 2018 Nov 1; 6(2): 3070-86.
55. Tsetse A, Bonniord E, Appiah-Kubi P, Tweneboah-Kodua S. Performance Study of the Impact of Security on 802.11 ac Networks. Future Gener Comput Syst 2018 : 11-17. Cham, Switzerland: Springer; [cited 2022 July 1]. Available from: https://doi.org/10.1007/978-3-319-77028-4_3.
56. Yang W, Li C-d, Chang G-r, Yao Y, Shen X-m. The effect of P2P-based worm propagation in an IPv6. Procedia Eng. 2011; 15: 3637-41.
57. Taib AM, Othman NA, Hamid RS, Abd Halim IH. A Learning Kit on IPv6 Deployment and its Security Challenges for Neophytes. In 2019 21st International Conference on Advanced Communication Technology (ICACT) 2019 Feb 17: 419-424. IEEE.
58. Zou CC, Towsley D, Gong W, Cai S. Routing worm: A fast, selective attack worm based on ip address information. Workshop on Principles of Advanced and Distributed Simulation (PADS'05) 2005 Jun 1 (pp. 199-206). IEEE.
59. Goel JN, Mehtre BM. Dynamic IPv6 activation based defense for IPv6 router advertisement flooding (DoS) attack. In 2014 IEEE International Conference on Computational Intelligence and Computing Research 2014 Dec 18 (pp. 1-5). IEEE.
60. Polčák L, Holkovič M, Matoušek P. A new approach for detection of host identity in IPv6 networks. In2013 International Conference on Data Communication Networking (DCNET) 2013 Jul 29 (pp. 1-7). IEEE.
61. Li C, Wu Q, Li H, Zhou J. SDN-Ti: a general solution based on SDN to attacker traceback and identification in IPv6 networks. In ICC 2019-2019 IEEE International Conference on Communications (ICC) 2019 May 20 (pp. 1-7). IEEE.
62. Lu Y, Wang M, Huang P. An SDN-based authentication mechanism for securing neighbor discovery protocol in IPv6. Secur Commun Netw. 2017 Jan 1;2017.
63. Mehdizadeh A, Abdullah RS, Hashim F. Secure group communication scheme in wireless IPv6 networks: An experimental test-bed. In 2012 International Symposium on Communications and Information Technologies (ISCIT) 2012 Oct 2 (pp. 724-729). IEEE.
64. Shih CM, Kao SJ. Security Gateway for Accessing IPv6 WLAN. In 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR'06) 2006 Jul 10 (pp. 83-88). IEEE.
65. Misra S, Goswami S, Taneja C, Mukherjee A, Obaidat MS. A PKI adapted model for secure information dissemination in industrial control and automation 6LoWPANs. IEEE Access. 2015; 3: 875-89.
66. Oliveira LML, Rodrigues JJ, de Sousa AF, Denisov VM. Network admission control solution for 6LoWPAN networks based on symmetric key mechanisms. IEEE Trans Industr Inform. 2016; 12(6): 2186-95.
67. Wang X, Mu Y. A secure mobility support scheme for 6LoWPAN wireless sensor networks. Secur Commun Netw. 2014; 7(3): 641-52.
68. Wallgren L, Raza S, Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. Int. J Distrib Sens Netw. 2013 Aug 22;9(8):794326.
69. Abdulla S. A neuro-fuzzy system to detect IPv6 router alert option DoS packets. Int Arab J Inf Technol. 2020; 17(1): 16-25.
70. Shiranzaei, A., Khan, R.Z. IPv6 Security Issues—A Systematic Review. In: Lobiyal D, Mansotra V, Singh U, editors. Adv Intell Syst Comput. Springer; 2017. p. 41–49.
71. Sajjad MM, Jayalath D, Bernardos CJ. A comprehensive review of enhancements and prospects of fast handovers for mobile IPv6 protocol. IEEE Access. 2018; 7: 4948-78.
72. Labs A. IPv6 Capable Rate by country (%) 2020 [Available from: https://stats.labs.apnic.net/ipv6.
73. Lencse G, Kadobayashi Y. Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64. Comput Secur. 2018; 77: 397-411.

المشاكل الأمنية في IPv6: مراجعة منهجية وفقًا لإرشادات PRISMA

شبير عبد الكريم عبد الله[1] **أحمد عبد الإله العاشور**[2]

[1]جامعة السلطان قابوس، مسقط، سلطنة عمان
[2]جامعة البصرة، البصرة، العراق

الخلاصة:

بما أن الإصدار 6 من بروتوكول الإنترنت (IPv6) عبارة عن تقنية جديدة ، فإن الثغرات الأمنية التي تنشأ خلال إعدادات شبكات الحاسوب هو أمر حتمي بسبب قلة المعرفة بهذه التقنية الجديدة ، ساهم الباحثون عبر العالم كثيرًا في نشر المعرفة حول الثغرات الأمنية في IPv6 وكيفية معالجتها على مدار العقدين الماضيين ، وفي هذه الدراسة ، يتم إجراء مراجعة منهجية للأدبيات لتحليل تقدم البحث في مجال أمان IPv6 باتباع عناصر التقارير المفضلة لطريقة المراجعة المنهجية والتحليل المسماة (PRISMA) ، تمت في هذه الورقة البحثية مراجعة ما مجموعه 427 دراسة من قاعدتي بيانات IEEE و Scopus ، و لتحقيق هدف الورقة البحثية ، فقد تم استخلاص العديد من عناصر البيانات الرئيسية من كل دراسة وتم إجراء نوعين من التحليل: التحليل الوصفي وتصنيف الأدبيات ، تُظهر نتائج البحث علامات إيجابية للمساهمات البحثية في هذا المجال ، ويمكن اعتباره هذه الورقة البحثية كمرجع لاستكشاف البحث في العقدين الماضيين في مجال أمان IPv6 ورسم الاتجاهات المستقبلية للبحوث في هذا المجال ، على سبيل المثال ، زادت نسبة النشر من 147 في العقد من 2000-2010 إلى 330 في العقد من 2011 إلى 2020 مما يعني أن النسبة المئوية للزيادة كانت 124٪. عدد الاستشهادات هو نتيجة رئيسية أخرى تعكس الاهتمام العالمي الكبير بالبحوث المخصصة لقضايا أمان IPv6 ، حيث كان 409 استشهاداً في العقد من 2000-2010 ، ثم ارتفع إلى 1643 استشهاداً خلال العقد من 2011 إلى 2020 ، أي أن نسبة الزيادة كانت 302٪.

الكلمات المفتاحية: IPv6 ، نشر IPv6 ، أمان IPv6 ، إرشادات PRISMA ، المراجعة المنهجية.