A Survey of Sybil Attack Countermeasures in IoT-based Wireless Sensor Networks

Akashah Arshad [1] , **Zurina Mohd Hanapi** [Corresp., 1] , **Shamala K. Subramaniam** [1] , **Rohaya Latip** [1]

[1] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, UPM Serdang, Selangor Darul Ehsan, Malaysia

Corresponding Author: Zurina Mohd Hanapi
Email address: zurinamh@upm.edu.my

Wireless sensor networks (WSN) have been among the most prevalent wireless innovations over the years, the exciting new Internet of Things (IoT) applications. IoT based WSN integrated with Internet Protocol (IP) allows any physical objects with sensors to be connected ubiquitous and send real-time data to the server connected to the Internet gate. Security in WSN remains an ongoing research trend that falls under the IoT paradigm. WSN node deployed in a hostile environment is likely to open security attacks such as Sybil due to its distributed architecture and network contention implemented in the routing protocol. In a Sybil attack, an adversary illegally advertises several false identities or a single identity that may occur at several locations called Sybil nodes. Therefore, in this paper, we give a survey of the most assuring methods up to date to defend from the Sybil attack. The Sybil attack countermeasure includes encryption, trust, received signal indicator (RSSI), encryption and swarm intelligence. Specifically, we survey different methods, along with their advantages and disadvantages, to mitigate the Sybil attack. We discussed the lesson learned and the future avenues of study and open issues in WSN security analysis.

1 # A Survey of Sybil Attack Countermeasures in IoT based
2 # Wireless Sensor Networks
3

5 Akashah Arshad[1], Zurina Mohd Hanapi [1], Shamala K. Subramaniam [2], Rohaya Latip [1],
6
7 [1] Department of Communication Technology and Network, Faculty of Computer Science and
8 Information Technology, University Putra Malaysia, Serdang 43400, Malaysia} [2] Sports
9 Academy, Universiti Putra Malaysia, Serdang 43400, Malaysia
10
11 Corresponding Author:
12 Akashah Arshad and Zurina Mohd Hanapi
13 Email address: akashah.arshad@gmail.com, zurinamh@upm.edu.my

15 ## ABSTRACT
16 Wireless sensor networks (WSN) have been among the most prevalent wireless innovations over
17 the years, the exciting new Internet of Things (IoT) applications. IoT based WSN integrated with
18 Internet Protocol (IP) allows any physical objects with sensors to be connected ubiquitous and
19 send real-time data to the server connected to the Internet gate. Security in WSN remains an
20 ongoing research trend that falls under the IoT paradigm.
21
22 WSN node deployed in a hostile environment is likely to open security attacks such as Sybil due
23 to its distributed architecture and network contention implemented in the routing protocol. In a
24 Sybil attack, an adversary illegally advertises several false identities or a single identity that may
25 occur at several locations called Sybil nodes.
26
27 Therefore, in this paper, we give a survey of the most assuring methods up to date to defend from
28 the Sybil attack. The Sybil attack countermeasure includes encryption, trust, received signal
29 indicator (RSSI), encryption and swarm intelligence.
30
31 Specifically, we survey different methods, along with their advantages and disadvantages, to
32 mitigate the Sybil attack. We discussed the lesson learned and the future avenues of study and
33 open issues in WSN security analysis.

35 ## INTRODUCTION
36 The Internet of Things (IoT) gained universal acceptance due to many applications for personal
37 use and the community. IoT represented a collection of "Things" or embedded devices connected
38 using various wireless technologies such as private and public networks (Atzori, Iera, &

39 Morabito, 2010). Based on the application domain, IoT applications are classifiable into five
40 groups, for example, health care (Zeb, Islam, Zareei, Mamoon, & Mansoor, 2016); Ambarkar &
41 Shekokar, 2020), environmental (Kumari & Sahana, 2019; Behera et al., 2020; Zhuang et al.,
42 2019; Jawad, Nordin, & Gharghan, 2017), smart city (Santos, Jimenez, & Espinosa, 2019; Luo,
43 2019), commercial (G. Li et al., 2018; Khanna & Tomar, 2016), IoT based robotic (Roy
44 Chowdhury, 2017) and industry (M. Zhu et al., 2020).
45
46   Wireless sensor networks (WSNs) are essential subsets of the Internet of Things (IoT)
47 that have emerged as a core technology for a variety of data-centric applications. Almost all IoT
48 network concepts are derived from WSNs. Both terms can be confusing at times, and they have a
49 lot of similarities and differences between IoT and WSN (Pundir, Wazid, & Singh, 2020). IoT
50 based WSN integrated with Internet Protocol (IP) allows any physical objects with sensors to be
51 connected ubiquitous and send real-time data to the server connected to the internet gateway.
52 Sensor data is relayed to the base station and is saved in the cloud for future access (Ala'Anzy &
53 Othman, 2019; Sheron, Sridhar, Baskar, & Shakeel, 2020). IoT-based WSN devices are powered
54 by batteries that later can be replaced, which poses a significant challenge to application
55 designers. To address these constraints in an IoT-based WSN, significant research has been
56 conducted on managing network power consumption. Most existing research focuses on
57 extending the IoT network lifetime. The purpose of WSN is to gather data from the sensor node
58 in the predetermine or random location and transmit the sensed data back to the base station.
59
60   The cumulative confirmed COVID-19 cases between 22 January and 12 October 2020
61 has reached 38,789,204 confirmed cases and has resulted in 1,095,097 deaths globally, as
62 reported by WHO (2020). As a result, the need for monitoring systems is in great demand. The
63 health of COVID-19 patients will be monitor continuously in an isolated room. Six per cent of
64 them need to warded in the Intensive Care Unit (ICU) to save their lives, as reported by El-
65 Rashidy et al. (2020).
66
67   Gupta et al. (2020) foresee that smart sensors, actuators, devices, and data-driven
68 applications can enable smart connected communities to strengthen the nations' health and
69 economic postures to combat current Covid-19 and future pandemics efficiently. Flying drones
70 regulated the quarantine and wearing of masks for public surveillance. Indoor isolation is made
71 more accessible by robots and digital assistants. With the help of aware IoT devices, it is possible
72 to track the origins of epidemics and ensure that patients follow important medical advice., as
73 highlighted by Fedele & Merenda (2020). However, from a security perspective, IoT networks
74 are prone to sensor-based attacks based on a recent survey conducted by Sikder et al. (2018). The
75 authors also addressed IoT devices' vulnerability to sensor-based threats due to the lack of
76 enough protection mechanisms to monitor the use of sensors by applications. An attack can be a
77 launch to the IoT based health application use to monitor COVID-19 patient. This security attack
78 can put the patient's life in danger, where the attacker can manipulate the medical IoT devices.

79

80   Also, attackers can execute out local-scale attacks on individual critical devices that
81 could include human life, such as the 2011 Stuxnet attack (Kushner, 2013), the late 2015 power-
82 grid blackout of Ukraine (Dvorkin Yury, 2020), the 2015 Jeep Cherokee attack (Schneider
83 David, 2015), the 2017 Brickerbot attack (Radware, 2017) and the 2018 Philips lightbulbs attack
84 demonstration. In a world where every device is connected to IoT, these attacks have shown how
85 catastrophic and diversified cybercrimes could be. Therefore, it is vital to detect Sybil attackers
86 in WSN to prevent their malicious activities. In other words, Sybil attacks present a significant
87 challenge for WSN, and improved defence mechanisms are required. We believe that the
88 conducted survey work will help the researchers in this Sybil countermeasures in WSN.

89

90   The recent survey covers the existing countermeasures to mitigate the WSN and IoT
91 security attack (Bhushan & Sahoo, 2017). There is a literature review focus on Sybil attack
92 countermeasures highlighted by Vasudeva & Sood (2018), Benkhelifaet et al. (2018) and
93 Gunturu (2015) and its comparison shown in Table 1. A reader interested in Sybil
94 countermeasures in an online network can read the following survey (Al-Qurishi et al., 2017;
95 Alharbi, Zohdy, Debnath, Olawoyin, & Corser, 2018). However, there is no previous literature
96 that reports cover any Sybil countermeasures based on swarm intelligence to the best of our
97 knowledge. This paper provides a general review of up-to-date countermeasures use to mitigate
98 the Sybil attack.   Also, advantages, limitations and whether the existing proposed method is IoT
99 ready are discussed.

100

101   The remainder of this paper is organized as follows. The "Survey Methodology" section
102 illustrates the approach and methodology used in this literature review on the Sybil attack. In
103 "Security Attack", we give a general overview of the Sybil attack. Next, we present the existing
104 Sybil attack countermeasures in "Sybil attack countermeasures". In "Discussion", we discuss the
105 comparisons on Sybil countermeasures in WSN and IoT. Section Finally, in "Conclusions", we
106 conclude the survey by summarizing the paper and outlining future research directions.

107

SURVEY METHODOLOGY

109 A systematic literature review (SLR) was carried out to examine countermeasures suggested by
110 previous research studies to thwart Sybil's attack with the Kitchenham (2004) benchmark,
111 emphasising previous work related to countermeasures for attacks on Sybil. This research
112 approach originated in the medical field to provide adequate knowledge for a repeatable study
113 method (Charband & Jafari Navimipour, 2016; Jafari Navimipour & Charband, 2016; Kupiainen,
114 Mäntylä, & Itkonen, 2015).To guide the reader on why we need to focus on the Sybil attack, to
115 discuss Sybil's critical principles and countermeasures as formalized in the following
116 subsections, we chose four research questions.

117

Research Questions

The questions in this section were aimed at identifying the main issues and challenges along with countermeasures used for attacks by Sybil, including efficiency, end-to-end delay, overhead, packet delivery ratio, detection metrics for Sybil attacks. This survey tries to address the following research questions (RQs), as shown in Table 2:

- RQ1: What is Sybil Attack?
- RQ2: Why is it to focus on Sybil IoT-based WSN environment? These two questions will prove the intent of countermeasure for Sybil Attack.
- RQ3: Where will new researchers concentrate on other methods of tackling the attack on Sybil? This problem aims to help the researcher focus on setting the direction of the proposed method.
- RQ4: How can the Sybil countermeasures achieve more robust algorithms to counteract those attacks?

This research question aims to explain how countermeasures are used to thwart Sybil's attack in achieving better algorithms, identifying challenges and techniques. The study needs are established after conducting a search query using suitable keywords, coming up with research questions, identifying the selection criteria, identifying the data retrieval, and conducting the quality evaluation. The aim of the survey could offer prepared answer and enlightenment for new researchers.

Survey Plan and Organization

The articles in this survey were acquired from most respected academic journals and also selected according to the checklist provided in (Kitchenham et al., 2009; Vasudeva & Sood, 2018b) for the quality evaluation. The research articles are acquired included IEEE, Elsevier, Springer, ACM, Wiley and MDPI, as these provided in-depth analysis. We started by filtering article by analysing the titles and abstracts. The entire research article is reviewed when the detailed information was not in the abstract. Hence articles are selected in this analysis based on a detailed inquiry into the nature of their material and documents. This in-depth work enables us to have a consistent and thorough understanding of the countermeasures for Sybil in the IoT-based environment.

The paper analysis was undertaken between late January 2015 and July 2020 for the first filtering. Boolean functions (OR, AND) and specific keywords detailed by synonyms and alternative spellings were used to investigate hundreds of papers in this area further.

("Sybil") and ("attack" or "attacks")

157   Next, papers are filtered again to acquire papers more accurately related to the review
158 context. The filtering process is to guarantee that no papers were overlooked in our review using
159 the keywords search below:
160
161 ("Sybil") and ("attack" or "attacks") and (IoT OR "internet of things") and (WSN OR "wireless
162 sensor networks") -"book" -"conference"
163

Eligibility Criteria

164
165 Articles were evaluated based on the Quality Assessment Checklist (QAC) to be selected in our
166 survey review list (Kitchenham et al., 2009; Vasudeva & Sood, 2018b). The articles in this
167 review that matched the research aim and objectives are selected according to the following
168 criteria:
169   • Does the study paper identify the Sybil attack countermeasure methods?
170   • Is the methodology listed in the research paper?
171   • Do testing methodologies use the resources available for re-implementation
172   (simulation or real system)?
173   • Does the research paper focus on WSN?
174   • Is the evaluation analysis done appropriately?
175 If "yes," the papers are chosen after the following conditions have been met:
176   • Any article that meets the criteria provided when there is a match in the keywords,
177   the article is selected
178   • The article is filtered after gone through the abstract and later will be recorded in the
179   final list
180   • Articles related to the countermeasure of the attack on Sybil will be included.
181

Data Filtration and Quality Evaluation

182
183 The search engine for Google scholars was used to locate the primary studies with the automated
184 search. The search led to the discovery of 28,800 articles that were considered significant for the
185 study. Data for all publications cited, abstracts and keywords of all articles are further analysed
186 in an Excel sheet. Through three articles resulting from the initial search, phase by phase. In this
187 segment, we search for keywords automatically and then find 372 journal articles and conference
188 papers. Then, we include the year range 2010-2020, which is reduced to 333 journals. Then,
189 we choose six famous publishers; 186 articles have been selected. Next, we checked whether any
190 research papers satisfied the criteria or were ignored. When the abstract was found to be
191 inadequate, the entire article was then checked, considering the requirements for inclusion or
192 exclusion given above (Kitchenham et al., 2009). Then, according to the publication time, the
193 number of 28 articles were selected and analysed. Fig. 1 illustrate the procedure used to choose
194 the articles for review. Researchers and scholars mostly published their contributions in the
195 established journal. Hence, conference papers have been excluded from this survey.

Security Attack

Generally, the security attack can be classified based on the attacker's objective, on which layer the attack is carried out. The method of attack reviewed in the previous literature is shown in Fig. 2. Firstly, objective-based security attack can be divided into the passive and active attack. A passive attack can bring down the network, eavesdropping to collect personal information, node destruction, and node malfunction. In an active attack, the attacker has the objective to take down the targeted network to become useless. Several examples of active attacks can be further classified into flooding, jamming, Denial-of-Service (DoS), black hole, sinkhole, Sybil and wormhole. Secondly, the various passive and active attacks in WSN and IoT can be categorised according to OSI layers (Butun, Osterberg, & Song, 2020; Farjamnia, Gasimov, & Kazimov, 2019). Different types of attack in the IoT environment are described in (Ahmad & Salah, 2017). Usman & Gutierrez (2018) categorized the author focus on wormhole attack and as well as other attacks are reviewed in (Farjamnia et al., 2019). Finally, the attack is categorized according to the attack method and how the malicious node can achieve its objective. Besides, the author also highlighted the mitigation strategies against security attacks in Pervasive and Mobile Computing. Sybil, DoS, hello and sinkhole are layered network attacks in WSN that are still relevant in IoT environments (Aufner, 2019). Thus, it is applicable to any IoT devices which uses the communication layer to communicate.

Based on the earlier discussion on the attack, the countermeasures of security attack consist of prevention, detection, and mitigation. Firstly, the prevention method's main objective is to hinder the malicious attack from taking place in the first place. Secondly, the detection countermeasures that able to detect when there is a security breach in the network. The countermeasure method can identify the type of attack and launch the mitigation solution to reduce the damage done by malicious activity, as highlighted in Fig. 3. Hence, the mitigation method is the steps taken to reduce the aftereffect of a security attack. Those three components are a complete protection framework and cannot be considered separately in defence of WSNs and IoT against different types of attacks, as highlighted in (Butun et al., 2020).

Such security attacks cause serious vulnerabilities to be routed inside the underlying network. Many attacks are less extreme, and others more severe (Md Zin, Badrul Anuar, Mat Kiah, & Ahmedy, 2015). One of the first attacks in the WSN environment is the Sybil attack, leading to further security attack as a black hole and wormhole, as highlighted by Murali & Jamalipour (2020). These attacks can interrupt the operation of WSN, which considers as IoT devices from collecting data sensors then stored in the cloud. Later, disruption caused IoT application like smart building, which houses many companies, to go haywire. Hence, this review paper focuses on the countermeasure method for Sybil and attack, which will be discussed later in the next section.

234 **Sybil Attack**

235 Sybil attack is defined by Newsome et al. (2002) when the malicious node can fake its own
236 identity during an attack or stole the identity from working valid nodes. Sybil attack utilises fake
237 identities to send false information, as highlighted by Romadhani et al. (2017) and Zhang et al.
238 (2005). In an ad-hoc network, Sybil attack that utilises multiple fake identities are discussed in
239 Lv et al. (2008). In geographic routing, fake identities exist in the network with faked locations
240 explored by Sha et al. (2013) and García-Otero et al. (2010), as shown in Fig. 4. Alternatively, a
241 high-resource Sybil Attack can participate in the selection process by listening and transmitting
242 its fake location during the protocol handshakes. Newsome et al. (2004) highlighted
243 countermeasures for Sybil Attack, namely radio testing and random key pre-distribution.
244 However, the author did not mention any limitation of the sensor network based on the listed
245 method. Goyal et al. (2015) and John et al. (2015) classified the Sybil Attack into a few
246 countermeasures categories.
247

248   An attacker tries to get more attention from nearby nodes in this attack to intercept data
249 packets. An attack that affects the process of packet delivery is routed are called routing attacks.
250 The simplest routing attack type is an altering attack in which the attacker modifies the routing
251 information by creating routing loops or fake error messages, as highlighted in Mosenia & Jha
252 (2017).
253

254   WSN security strategies can be broken down into two categories: prevention-based and
255 detection-based. Due to restricted resources and a broadcast medium, mitigation methods such as
256 encryption are challenging for WSNs. Also, all possible attacks will not be protected by the
257 suggested cryptographic solutions. An attacker can easily obtain the symmetric key. The whole
258 network is compromised since the attacker will decrypt all encrypted data using the symmetric
259 key. The second line of defence is called the Intrusion Detection System (IDS), is important to
260 detect malicious parties that try to use the weakness in the security and potential insecurities and
261 detect the attacks that have not been detected before (Hidoussi et al., 2015).
262

263 WSN nodes are deployed in the environment without any supervision. The unattended nature of
264 WSNs, adversaries, can readily produce such blackholes attack. Severely compromised node and
265 DOS attacks can interfere with the standard data delivery between sensor nodes and sink or even
266 partition the topology, as Shu et al. (2010) highlighted. In the next chapter, we will address the
267 Sybil Attack countermeasures suggested by the previous researchers.

268 **Sybil Attack Countermeasures**

269 In this section, the countermeasures used to mitigate the Sybil attack can jeopardize humans'
270 lives by monitoring IoT medical devices or other critical IoT applications. Radio resource testing
271 (RTT) is a countermeasure that can distinguish direct forms of Sybil attack Balachandran &

272 Sanyal (2012). Newsome et al. (2004) stated that resource testing is the popular countermeasure
273 to lower the probability of being attack rather than eliminating Sybil attacks for good. Ssu,
274 Wang, & Chang (2009) proposed the RTT mechanism that assumed nodes in the network could
275 not transmit and receive. Also, Douceur (2007) has proven that a trusted certification method can
276 eliminate the Sybil Attack using a central authority. Some researchers proposed that key
277 management (Paul, Sinha, & Pal, 2013; Zhang et al., 2005; Eschenauer & Gligor, 2002) or
278 encryption for authentication using asymmetric key cryptography which is not suitable due to
279 higher overhead and not scalable (Boneh & Franklin, 2001; Zhu et al. (2006). Ssu et al. (2009).
280 Other methods include Sybil Attacker detecting by verifying neighbouring nodes' set, which
281 caused higher communication overhead. Software-based attestation is a method where the
282 verifier performs through various software or hardware challenges against its neighbouring node
283 (Steiner & Lupu, 2016).

284

285 The radio signal is susceptible to the interference dan signal attenuation caused by the
286 surrounding, which influences the precision of detecting a malicious node using RSSI-based and
287 Time Difference of Arrival-based Scheme(TDOA) based countermeasures. Chan et al. (1994)
288 proposed two localisation methods, namely the estimation of TDOA and solving hyperbolic
289 position. Wen et al. (2008) explained the TDOA ratio with the sender's identity. A Sybil is
290 detected once the beacon nodes calculated and find the same TDOA ratio for two different
291 identities. These countermeasures are no longer in trend as many researchers currently moving
292 towards the proposed method, as shown in Fig. 5. In most current literature, researchers focus on
293 encryption and RSSI mechanisms that 29% of the solution provided for Sybil countermeasures.
294 The rest of the solutions accounted for 14%, 14% and 7 % for trust, artificial intelligence and
295 encryption hybrid. Lastly, 3% and 4% are accounted for rule-based anomaly and multi-kernel.

296

297 Li & Cheffena (2019) proposed a multi-Kernel based expectation-maximization (MKEM)
298 countermeasure for Sybil attacks. The innovative countermeasure analyses the radio resource of
299 the sensor node to produce channel vectors. These channel vectors are comprised of the power
300 gain and delay spread of the channel impulse response extracted out from the received packet of
301 the sensor node. In addition, gap statistical analysis method to validate and EM method to
302 summarize the detection results.

303

304 **Cryptography**

305

306 Cryptography is a popular research area for WSN just before the IoT becomes the technological
307 trend. Although cryptography requires lots of processing power, there is still an ongoing research
308 area among researchers. Kouicem et al. (2018) highlighted two fundamental distribution
309 approaches: key deterministic and Probabilistic key distribution. In deterministic approaches, to
310 provide maximum security coverage connection, each entity can make a secure link to others.
311 However, the key management protocol becomes defenceless when under a security attack. Also,

312   Paul et al. (2013) highlighted three types of cryptographic technique: creating and managing,
313   distributing, and validating keys for identities. Firstly, Symmetric key distribution is a method
314   using a similar key is utilised for encryption and decryption of the messages, namely Encryption
315   Standard (AES), Rivest Cipher 4(RC4) and Triple Data Encryption Standard (3DES). However,
316   key management problems and scalability issues are the main disadvantages of the symmetric
317   key. WSN nodes are powered by batteries that are not suitable for implementing public-key
318   cryptography due to high processing power and high network load when generating keys,
319   distributing key, and maintaining key. Devices equipped with cryptographic is more likely to
320   expose to brute force attack. Asymmetric key distribution utilised public key for encryption
321   while the private key utilised for decryption.
322
323   Jain et al. (2020) proposed a node authentication method for wireless sensor node to
324   avoid security attacks and provide secure communication channels. The base station is
325   responsible for generating the random value and a secret value to distribute among the sensor
326   nodes. Each node is responsible for storing its secret and random value.Zhang & Zhou (2010)
327   proposed using the Markle hash tree, trust values and message authentication codes for location
328   verification algorithm. This approach works well with networks that are organized in a tree or
329   hierarchical structure. This method falls in the encryption hybrid taxonomy shown in the
330   previous pie chart diagram. Claycomb & Shin (2011) proposed a method based on a security
331   policy that utilized key establishment to combine group-based distribution model and identity-
332   based encryption. He et al. (2011) proposed combining the merits of both public and symmetric
333   cryptographic methods for key management in WSNs, that each node is configured with a public
334   key system to establish end-to-end symmetric keys with other nodes like EDDK.
335
336   Dong & Liu (2012) proposed a scheme that deploys auxiliary nodes to execute the key
337   establishment to help key establishment between sensor nodes. This method utilizes a secured
338   Fuzzy Clustering Algorithm to determine the nodes that securely join the cluster. The cluster
339   head oversees routing based on criteria, trust value and energy. Kim & Kim (2013) proposed a
340   scalable and robust hierarchical key establishment scheme that enhances resilience against node
341   capture, traffic analysis, and acknowledgement spoofing attack. In addition, this scheme provides
342   periodic critical updates without communication costs for key transport.Razaque & Rizvi (2017)
343   proposed a method to combat the Sybil attack, which comprises two novel algorithms. The first
344   algorithm fragments the data to avoid detection from the malicious node. The second algorithm
345   aims to provide authentication for nodes joining the network through encryption.
346
347
348   **Received Signal Strength Indicator**
349   Received Signal Strength Indicator (RSSI) has been used to sense Sybil attack and accounted for
350   about 26% in Fig. 5. RSSI remains the choice of researchers to mitigate against Sybil attack
351   because it does not require special hardware to approximate the location of neighbours. There are

352   many different approaches in RSSI to counter-attack and which varied between researcher.

353   Demirbas et al. (2006) proposed a countermeasure method Sybil attack by only two receivers. To

354   improve accuracy, Wang et al. (2007) came up with a countermeasure using RSSI from multiple

355   neighbours instead of two neighbour nodes. Also, the status message can be used to validate the

356   location in the hierarchical network that utilises Jake Channel. Zhong et al. (2004) proposed the

357   location verification based on RSSI signal using four or more detector nodes to detect the signals

358   that can verify a node's location.

359

360   Lv et al. (2008) proposed a method for stationary wireless sensor networks called

361   Cooperative Received Signal Strength (RSS) based Sybil Detection (CRSD) to estimate the

362   distance between two identities and to locate the correlation of location between the unique

363   identities of multiple neighbouring nodes. Lazos et al. (2005) proposed a method that utilises the

364   target node to determine its position using beacon information transmitted by both benevolent

365   and malicious anchor nodes.

366

367   García-Otero et al. (2010) proposed innovative and lightweight location verification

368   methods to detect and isolate Sybil attack. The distributed trust model is integrated with the

369   routing protocol mainly to defence from routing attack. Abbas et al. (2013) utilise one

370   neighbouring node to detect RSS in mobile environments. In Secure and Scalable Geographic,

371   Opportunistic Routing with received signal strength (SGOR) is an opportunistic routing protocol

372   proposed by Lyu et al. (2015). This proposed trust method and a combination of calculating the

373   difference of distance beacon messages and RSSI to detect the malicious nodes' fake location and

374   defend against grey hole attack. The proposed method can defend from other attacks such as

375   rushing, wormhole, replay, and collusion. However, this method's limitation is when the attacker

376   has higher energy capacity and higher transmission power, which can easily deceive the sender

377   about its location. Kumari et al. (2017) provided a framework using authentication and RSSI

378   against Sybil attack. The RSS values are calculated from the arrival angle, stored in the database

379   at each node. The RSSI threshold value determines if the nodes fall within the safety zone and

380   the precautionary zone. Also, the ant colony optimisation method was used to determine the

381   optimized route for the packet to travel from source to destination. The second category assumes

382   that a node can occur at one location at a specific time. Raja et al. (2017) suggested another

383   encryption approach using the Fujisaki Okamoto (FO) algorithm and their implementations. FO

384   algorithm is an encryption method that offers a good defence against Sybil attacks by using ID-

385   based verification. In the proposed scheme, multiple performance metrics were analysed,

386   especially the high energy consumption is used as an indicator to sense Sybil attack in wireless

387   sensor networks.

388

389   Yuan et al. (2018) presented a lightweight Approximate Point-in Triangulation Test (SF-

390   APIT) algorithm that can pinpoint Sybil attacks in a wireless network in a distributed way using

391   a range of free and iterative refinement-based methods. The individual node implemented the

392   algorithm was based on RSS, which does not cost any overhead in WSN. Based on the node
393   location, the node utilises three beacons in the triangulation method to calculate the possible
394   combination overlapped triangle region, which can estimate the unknown node's location.
395   Therefore, the centroid of the overlapping area is considered as the approximate location of this
396   node. Giri et al. (2020) proposed a countermeasure that protects the beacon node from Sybil
397   attack by implementing the information-theoretic approach. Any localization algorithm can use
398   this approach to provide protected localization in WSNs for the Sybil attack. Liu (2020)
399   proposed an improved RSSI-based Sybil Attack Detection Scheme in Wireless Sensor Networks.
400   The proposed method able to quickly detect malicious nodes with minimum energy
401   consumption.
402
403   The hierarchical topology of cluster network has many advantages in energy efficiency
404   due to less communication, scalability, and routing. In addition, the proposed method utilised
405   both RSSI and CSI to protect the hierarchical cluster network from Sybil attack. Jamshidi et al.
406   (2019) proposed a lightweight method that consists of two algorithms for detecting Sybil node
407   masquerading as cluster heads and cluster members. Sarigiannidis et al. (2015) proposed a
408   secure communication mechanism for clustered WSNs based on the elliptic curve cryptography
409   (ECC) that allows end-users to recover data collected confidentiality. The proposed method has a
410   firm reliance on historical records, making this approach not stable and durable. Angappan et al.
411   (2020) proposed a localized scheme for Sybil node detection called NoSad using RSSI value and
412   the intra-cluster communication, which can be deployed to the device. However, NoSad is not
413   stable when there is a minimum of two Sybil node and cannot cater to mobility in WSN.
414
415   Jan et al. (2015) propose an innovative detection countermeasure for Sybil attack in a centralized
416   clustering-based hierarchical network. Sybil nodes with fake identities are detected before the
417   cluster to ensure that usage of the resources is optimized. The detection of Sybil nodes is achieved
418   by analysing the received signal strength from any two high energy nodes. Wang et al. (2018)
419   proposed a Sybil attack detection using Channel State Information (CSI) and a self-adaptive
420   multiple signal classification algorithm RSSI for dynamic and static nodes in the clustered
421   network.
422
423   **Trust**
424   According to Ishmanov et al. (2017), there is not much research done on security attack detection
425   based on unrelated criteria such as packet drop and packet modification. Mawgoud et al. (2020)
426   highlighted that trust could be set up automatically without personal interaction with previously
427   unregistered and unknown peer neighbours in typical IoT scenarios.
428
429   Karlof & Wagner (2003) highlighted that the trust centre uses a key shared between two
430   nodes for node verification to secure the network. Zhan, Shi, & Deng (2012) proposed the trust
431   management and encryption method that can detect and guess the future behaviour of Sybil

432   Attacker. During next-hop selection, this trust information is vital to select a safe path to the
433   destination.

434

435   Zhan et al. (2012) proposed selecting the next hop based on trust and energy criteria. The
436   energy watcher module calculates the energy cost for neighbouring nodes and the node's energy,
437   where this information stored in the neighbourhood table. The energy watcher module also
438   approximates the average energy required to route the packet from sender to destination. Alsaedi
439   et al. (2017) proposed a method to detect Sybil attack based on name, location and energy
440   information for each time a new message was routed to the sender. The proposed method also
441   uses a multi-level system where each rule to recognise a Sybil attacker is given to specific
442   agents. These Sybil attackers engage in data aggregation at different stages to collude the
443   aggregated data to disclose invalid data. Also, these malicious nodes may modify and tamper
444   with the timestamps of a message with multiple identities, which can cause havoc to synchronise
445   local clocks in IoT devices. Maddar et al. (2017)   proposed an innovative detection method for
446   Sybil nodes with fake identities before the cluster formation in a centralized clustering-based
447   hierarchical network to optimize the usage of the resources. The detection countermeasure works
448   by analyzing neighbouring nodes the received signal strength. Jinhui et al. (2018) proposed a
449   method that can effectively predict energy consumption and increase the detection rate to detect
450   malicious nodes.

451

452

453   Liu et al. (2007) explained that landmarks are required to be trusted. All routing protocols
454   are related to their mechanism of localisation and cannot be isolated from them. Garcia et al.
455   proposed a lightweight method that consists of localisation and intrusion identification
456   techniques using distrusted trust model to thwart several security attacks.Prathusha et al. (2017)
457   proposed secure geographic routing (GSR), which is have been modified from SecuTPGF.
458   GSR's advantage is that it uses low computational power to combat security attacks such as
459   spoofing and an assault on Sybil by introducing SHA-3 node and message authentication. Zhou
460   et al. (2015) proposed a watchdog method that implements energy consumption optimisation
461   while providing just enough security. The validation technique through a watchdog mechanism
462   able to defend against Sybil attack.

463

464

465   **Artificial Intelligent**
466   Intrusion detection systems are the example of artificial intelligence applications in the
467   cybersecurity field. Cybersecurity solutions can distinguish between legitimate or malicious node
468   through detailed traffic analysis Cyberattacks were first detected with rule-based systems, which
469   could detect attacks based on their signatures at the beginning of the Internet. Swarm Intelligence
470   (SI) is a subdivision of artificial intelligence where the inspiration of this algorithm mimics
471   biological swarms' intelligent behaviour in solving and simulating real problems. The SI
472   algorithms are intended to investigate the concepts of simple individuals who can display
473   sophisticated and complex swarm optimization behaviours through collaboration, organisation,

474 knowledge exchange, and learning between swarm members.(Kolias, Kambourakis, &
475 Maragoudakis, 2011). These swarm intelligences can be categorized according to the year when
476 they are invented. Particle Swarm Optimization and Ant Colony Optimization was invented before
477 the year 2000. Artificial Fish Swarm and Bacterial Foraging Optimization need further
478 development to enhance, and Firefly Optimization and Artificial Bee Colony optimization are
479 widely used optimization during the year 2000 until 2010. Pigeon inspired optimization, Grey wolf
480 optimizer, and Butterfly optimization algorithm require further development.
481

482   Prithi & Sumathi (2020) proposed a method called Learning Dynamic Deterministic Finite
483 Automata (LD^{2}FA) and Particle Swarm Optimization (PSO) for intrusion detection, and the data
484 is transmitted securely over-optimized path. LD2FA-PSO got a 16% increase in throughput than
485 cluster-based IDS, almost 70% rise in throughput than lightweight IDS, 6% and 32% increment
486 in network lifetime over PSO and GLBCA, respectively; almost 30% and 54% improve in network
487 lifetime over GA and LDC, respectively. The energy consumed is almost 3% and 6% lesser than
488 PSO and GA, and 13% higher energy is consumed than LDC.
489

490   Raghav et al. (2020) used swarm intelligence algorithms based on the bee to provide a
491 secure routing scheme. The proposed routing mechanism utilize primary scout bee and secondary
492 scout bee to carried out the secured and optimized routing. In many scenarios, it improves data
493 efficiency while also providing security against flood, spoof, and Sybil attacks. Its disadvantages
494 include that when the solution is close to the global optimum, it is possible to get stuck in the local
495 optimum, resulting in stagnation.
496
497

498 **Discussion**

499 This paper has reviewed the countermeasures used to defence against Sybil attack. Table 3
500 provides a comparative summary of the proposed method to countermeasure against Sybil attack
501 in term of its advantage, limitation, scalability readiness and classification of detection,
502 prevention. Besides security, scalability is also essential for deploying many devices under the
503 IoT paradigm to become a major success (Arellanes & Lau, 2020). Security countermeasures
504 should expand to many sensor nodes and intelligent devices (Lu & Xu, 2019). Comparing the
505 proposed method will help the future researcher evaluate and identify any research gap that will
506 help them innovate or develop new countermeasures in the future. The proposed method to
507 combat Sybil attack is the random key pre-distribution, cryptographic method, radio resource
508 testing, received signal strength indicator (RSSI) localisation techniques, time difference of
509 arrival (TDOA) localisation technique, neighbouring node information, Trust, watchdog, RFID,
510 clustering, and geographic routing.
511

512   Sybil attack countermeasures are of the simplified method due to the neighbouring node,
513 and trust information is exchanges of control message between one or more nodes so that the
514 sender can validate the identity of its neighbouring nodes. Also, this information is used as

515 criteria's in selecting the best route from the sender to the destination nodes. Watchdog is used to
516 monitor the neighbouring nodes in a centralised or decentralised scheme using the physical and
517 data link layer. This information is used in selecting the best route for multi-hop routing.
518
519   Cryptographic and random key pre-distribution is implemented in the application layer,
520 where its encryption and decryption process utilises the processing and memory resources.
521 However, this authentication using asymmetric key cryptography has a higher overhead and not
522 scalable. Also, the encryption process requires high computation and memory resources for the
523 cryptography method and its attributes. The limitation for pre-distribution of the key. However,
524 the proposed method utilises high computational overhead, computational delays and a high load
525 of control messages transmitted to nodes. Keys are store in databases that are vulnerable to
526 attacks. One of the significant challenges is developing a lightweight key delivery network for
527 sensor nodes with limited resources to support numerous protocols, applications and services at
528 all IoT layers levels (B. B. Gupta & Quamara, 2018).
529
530   Radio resource testing, RSSI and TDOA measure the physical layers described by Almas
531 Shehni et al. (2017) for the Sybil attack. RSSI and TDOA are two methods to locate Sybil Attack
532 by measuring signal strength and the distance between beacons. The RSSI method used less
533 energy than other methods and did not require any special requirements or additional details.
534 According to the studies, the distances between nodes from the RSSI can be easily calculated
535 based on RSSI information. RSSI-countermeasure methods are popular among researchers to
536 detect Sybil Attack (Demirbas & Song, 2006). However, the limitation of RSSI are susceptible to
537 interference, environment factor, the need for a beacon node, receiver system delay, non-line of
538 sight transmission, and a malicious node with high power transmission could easily deceive the
539 good node with its fake location and identity. The disadvantage of TDOA is implemented in a
540 highly dense network which can cause false detection of an honest node being detected as an
541 attacker. An honest node's location is at the exact location as the detector node are the leading
542 cause of false detection. Also, an attacker with a directional antenna could easily overcome being
543 detected. These methods are not suitable for IoT devices that are mobile (Wu & Ma, 2019). RSSI
544 has some limitation where there is no line of sight communication due to the obstruction of
545 obstacle between a beacon node and a dumb node which caused the signal to get reflected from
546 the surroundings (Ren et al., 2007). Hence, from the summary of countermeasures proposed by
547 the previous researcher, the future researcher should use RSSI due to its energy efficiency. To
548 complement the limitation of RSSI, trust countermeasures based on energy due to energy
549 heterogeneity of IoT devices should be combined with RSSI to enable the detection of Sybil
550 malicious nodes.
551
552   Software attestation is a method where software routines that transmitted to the
553 neighbouring node for validation. These routines are stored inside the memory, and the
554 neighbouring nodes are required to respond to the challenge within specific criteria like integrity

555   validation in software and hardware, time duration, how software routine is read in the memory,
556   and the interaction method. For example, the radio resource testing technique extracts the battery
557   or energy level from these network devices. High energy devices are assumed to be malicious
558   attacker nodes. However, this approach can cause the communication overhead to increase due
559   to control packets for resource verification.
560

561   Fig. 6 illustrates the proposed method that the researcher has developed from the year
562   2010 until 2020. The statistical charts show an increase in the encryption and trust method
563   proposed by the researchers in 2017. In the year 2020, there is an increase in the proposed
564   method using RSSI and less focus on encryption. Most of the artificial intelligence scheme
565   proposed by the researchers in 2020 is used to optimize the routing process in complement with
566   security. Hence, in the next section future researcher should try to integrate artificial intelligence
567   to optimize the method such as cross layer, Software Defined Network (SDN), cross platform
568   intrusion detection and blockchain.
569

570

571   **Lesson learned and future direction**

572

573   WSN security is a hot research topic. There are many challenges and issues in WSN's security
574   which future researcher can explore and provide a new solution. Specific requirements and
575   constraints, such as low complexity and reliability, must be imposed on the provided solution.
576   This section briefly discusses lessons learned from the previously proposed method and possible
577   future directions for Sybil Attack countermeasures.

578

579   **Cross-layer**

580

581   Lesson learned: There is a possibility that an attack could be launch from the different layer
582   during the communication process. Hence, this requires security countermeasure to handle
583   cross-layer attacks and require access to all information from multiple layers. Significantly
584   through joint optimization of multiple network layers. Besides security, cross-layer information
585   also beneficial in term of optimizing energy efficiency

586

587   Dhivya Devi & Vidya (2019) discussed and explored the cross-layer design approaches
588   that have been in WSN. For example, some proposed methods implement a cross-layer in
589   detecting intrusion and routing (Fatema & Brad, 2013; Umar et al., 2017). The motivation to
590   implement cross-layer design due to it can optimise the network performance in the wireless
591   sensor. The cross-layer design allows the ease of exchanging information between layers, which
592   helps the WSN be energy efficient and increase QoS parameters. Based on the proposed method
593   for Sybil attack, countermeasures surveyed, not many works of literature in focusing security
594   attack. The method in detecting Sybil attack should incorporate the cross-layer approach to
595   increase accuracy in detecting security attacks. The future researcher can utilise the RSSI, which

596 lightweight from the physical layer with an upper layer such as Trust and Mobile agent for
597 detecting Sybil Attack. A cross-layer method for detecting Sybil attack with a mobile agent is
598 proposed by Gandhimathi (2016). Cross-layer allows sharing of information among the MAC
599 and networks layers is to optimise network performance. Also, this information can utilise by a
600 mobile agent to prevent a security attack. However, the proposed method to prevent Sybil attack
601 and another kind of attack increases the communication overhead.
602
603 **Software-Defined Network**
604
605 Lessons learned: SDN and SDMN are the current trending research topics for 5G communication
606 security. The exact security method for SDN and SDMN remain unexplored by researchers.
607 With the deployment of SDN and SDMN in the 5G communication, innovative techniques are
608 needed in this area.
609
610   Apart from novel security solutions for IoT, there is a developing trend of SDN that
611 allows reconfiguration of the network and central monitoring with possible centralised routing
612 algorithm. This emerging paradigm opens up the researcher's door to develop a lightweight
613 security framework running from the SDN controller, running at the central controller (Hameed,
614 Khan, & Hameed, 2019).
615
616 **Cross-Platform Intrusion Detection**
617
618 Lesson learned: The IoT has from WSN where the sensor nodes are assumed to homogenous
619 device with limited resources to heterogeneous devices with different capabilities but still limited
620 in energy constraints. Colom et al. (2018) highlighted in the survey that the current trend of IDS is
621 moving toward a universal and cross-platform method. The proposed method able to handle device
622 heterogeneity, scalability of IoT network and limitation.
623
624   Security and malware attack on the Internet could also be deployed in IoT due to various
625 protocols utilized at every layer in the heterogeneous devices. The interoperability issues and
626 lack of standard in IoT becomes a security challenge. Many IoT devices that launched in the
627 market have a security flaw due to that security was not the top priority and have not been
628 considered in the past. The previous IoT devices are lack authentication method or able to detect
629 or prevent an attack. A big challenge for Intrusion detection methods to be deployed in the IoT
630 environment is a big challenge due to the heterogeneity of devices. One example cross-platform
631 intrusion detection; an innovative home application must retrieve information from personal
632 healthcare sensing with a secure connection. Therefore, we need a quick, efficient and robust
633 intrusion detection countermeasure to provide an undisruptive and continuous connection to
634 multiple IoT platforms.
635

636 **Blockchain**

637

638 Lesson learned: Blockchain is the latest decentralised distributed system technology designed
639 and invented by Bayer et al. in 1992. Proof of work, asymmetric cryptography, electronic
640 signatures, and hash functions are all used in blockchain technology (Lazrag, Chehri, Saadane, &
641 Rahmani, 2020).

642

643   WSN sensor nodes are distributed and placed in an extreme and complex environment, so
644 it is crucial to implement secure authentication between sensor nodes in WSN(Cui et al., 2020).
645 Blockchain is suitable for IoT with a hierarchical topology that has limited memory,
646 computation, and energy. Merkle trees were incorporated into blockchain technology to provide
647 efficient and reliable digital timestamps (Dorri et al., 2017). Blockchain has been applied in the
648 security framework, and security countermeasure is still in the experimental phase, which will be
649 the future direction of the research (Mubarakali, 2021)

650

651 **Conclusions**

652 This paper discussed different countermeasures to defend the IoT-based WSN from the Sybil
653 attack launched from various application domains. We have expanded on their modus operandi,
654 advantages, and limitations of each countermeasure's categories. Although various researchers
655 have proposed several countermeasures, there is no efficient method to overcome most attacks
656 with complete geographic routing accuracy. Also, we have observed that the trust mechanism is
657 the most popular countermeasures for the Sybil attack from 2015 and 2020.
658 The new researcher should investigate developing a framework that is lightweight to secure IoT
659 network. Developing a secure framework for IoT, which consists of heterogeneous devices with
660 different wireless technologies, is challenging. The development of a security framework for
661 these IoT devices should consider IoT's scalability and resource constraint (Razacheema,
662 Alsmadi, & Ikki, 2018).

663

664

665

666 **Acknowledgements**
667 This work was supported by Geran Putra Berimpak Universiti Putra Malaysia (9659400).

668

669 **References**
670 Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). Lightweight sybil attack
671   detection in MANETs. *IEEE Systems Journal*, *7*(2), 236–248.
672   https://doi.org/10.1109/JSYST.2012.2221912
673 Ahmad, M., & Salah, K. (2017). IoT security : Review , blockchain solutions , and open
674   challenges. *Future Generation Computer Systems*.
675   https://doi.org/10.1016/j.future.2017.11.022
676 Al-Qurishi, M., Al-Rakhami, M., Alamri, A., AlRubaian, M., Rahman, S. M. M., & Hossain, M.

677   S. (2017). Sybil defense techniques in online social networks: A survey. *IEEE Access*, *5*,
678   1200–1219. https://doi.org/10.1109/ACCESS.2017.2656635

679   Ala'Anzy, M., & Othman, M. (2019). Load Balancing and Server Consolidation in Cloud
680   Computing Environments: A Meta-Study. *IEEE Access*, *7*, 141868–141887.
681   https://doi.org/10.1109/access.2019.2944420

682   Alharbi, A., Zohdy, M., Debnath, D., Olawoyin, R., & Corser, G. (2018). Sybil Attacks and
683   Defenses in Internet of Things and Mobile Social Networks. *International Journal of*
684   *Computer Science Issues*, *15*(6), 36–41.

685   Almas Shehni, R., Faez, K., Eshghi, F., & Kelarestaghi, M. (2017). A New Lightweight
686   Watchdog-Based Algorithm for Detecting Sybil Nodes in Mobile WSNs. *Future Internet*,
687   *10*(1), 1. https://doi.org/10.3390/fi10010001

688   Ambarkar, S. S., & Shekokar, N. (2020). Toward Smart and Secure IoT Based Healthcare
689   System (Vol. 266, pp. 283–303). Springer International Publishing.
690   https://doi.org/10.1007/978-3-030-39047-1_13

691   Angappan, A., Saravanabava, T. P., Sakthivel, P., & Vishvaksenan, K. S. (2020). Novel Sybil
692   attack detection using RSSI and neighbour information to ensure secure communication in
693   WSN. *Journal of Ambient Intelligence and Humanized Computing*, (0123456789).
694   https://doi.org/10.1007/s12652-020-02276-5

695   Arellanes, D., & Lau, K. K. (2020). Evaluating IoT service composition mechanisms for the
696   scalability of IoT systems. *Future Generation Computer Systems*, *108*, 827–848.
697   https://doi.org/10.1016/j.future.2020.02.073

698   Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer*
699   *Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

700   Aufner, P. (2019). The IoT security gap: a look down into the valley between threat models and
701   their implementation. *International Journal of Information Security*.
702   https://doi.org/10.1007/s10207-019-00445-y

703   Balachandran, N., & Sanyal, S. (2012). A Review of Techniques to Mitigate Sybil Attacks.
704   *International Journal of Advanced Networking and Applications*, *4*, 1–6.

705   Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., & Gandomi, A.
706   H. (2020). I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT-Based
707   Environmental Monitoring. *IEEE Internet of Things Journal*, *7*(1), 710–717.
708   https://doi.org/10.1109/JIOT.2019.2940988

709   Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges
710   in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE*
711   *Communications Surveys and Tutorials*, *20*(4), 3496–3509.
712   https://doi.org/10.1109/COMST.2018.2844742

713   Bhushan, B., & Sahoo, G. (2017). Recent Advances in Attacks , Technical Challenges ,
714   Vulnerabilities and Their Countermeasures in Wireless. *Wireless Personal*
715   *Communications*. https://doi.org/10.1007/s11277-017-4962-0

716   Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. In
717   *Advances in the Astronautical Sciences* (Vol. 102 I, pp. 213–229). https://doi.org/10.1007/3-
718   540-44647-8_13

719   Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities,
720   Attacks, and Countermeasures. *IEEE Communications Surveys and Tutorials*, *22*(1), 616–
721   644. https://doi.org/10.1109/COMST.2019.2953364

722   Chan, Y. T., & Ho, K. C. (1994). A simple and efficient estimator for hyperbolic location. *IEEE*

723   *Transactions on Signal Processing*, *42*(8), 1905–1915. https://doi.org/10.1109/78.301830

724   Claycomb, W. R., & Shin, D. (2011). A novel node level security policy framework for wireless

725   sensor networks. *Journal of Network and Computer Applications*, *34*(1), 418–428.

726   https://doi.org/10.1016/j.jnca.2010.03.004

727   Colom, J. F., Gil, D., Mora, H., Volckaert, B., & Jimeno, A. M. (2018). Scheduling framework

728   for distributed intrusion detection systems over heterogeneous network architectures.

729   *Journal of Network and Computer Applications*, *108*, 76–86.

730   https://doi.org/10.1016/j.jnca.2018.02.004

731   Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A Hybrid

732   BlockChain-Based Identity Authentication Scheme for Multi-WSN. *IEEE Transactions on*

733   *Services Computing*, *13*(2), 241–251. https://doi.org/10.1109/TSC.2020.2964537

734   Demirbas, M., & Song, Y. (2006). An RSSI-based scheme for sybil attack detection in wireless

735   sensor networks. *Proceedings - WoWMoM 2006: 2006 International Symposium on a*

736   *World of Wireless, Mobile and Multimedia Networks*, *2006*, 564–568.

737   https://doi.org/10.1109/WOWMOM.2006.27

738   Dhivya Devi, C., & Vidya, K. (2019). A Survey on Cross-Layer Design Approach for Secure

739   Wireless Sensor Networks. In *International Conference on Innovative Computing and*

740   *Communications* (Vol. 55, pp. 43–59). Springer Singapore. https://doi.org/10.1007/978-

741   981-13-2324-9_6

742   Dong, Q., & Liu, D. (2012). Using auxiliary sensors for pairwise key establishment in WSN.

743   *Transactions on Embedded Computing Systems*, *11*(3).

744   https://doi.org/10.1145/2345770.2345771

745   Douceur, J. R. (2007). The Sybil Attack, 251–260. https://doi.org/10.1007/3-540-45748-8_24

746   El-Rashidy, N., El-Sappagh, S., Islam, S. M. R., El-Bakry, H. M., & Abdelrazek, S. (2020). End-

747   To-End Deep Learning Framework for Coronavirus (COVID-19) Detection and

748   Monitoring. *Electronics*, *9*(9), 1439. https://doi.org/10.3390/electronics9091439

749   Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor

750   networks. *Proceedings of the 9th ACM Conference on Computer and Communications*

751   *Security - CCS '02*, 41. https://doi.org/10.1145/586115.586117

752   Farjamnia, G., Gasimov, Y., & Kazimov, C. (2019). Review of the Techniques Against the

753   Wormhole Attacks on Wireless Sensor Networks. *Wireless Personal Communications*,

754   *105*(4), 1561–1584. https://doi.org/10.1007/s11277-019-06160-0

755   Fatema, N., & Brad, R. (2013). Attacks and Counterattacks on Wireless Sensor Networks.

756   *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, *4*(6), 1–15.

757   https://doi.org/10.5121/ijasuc.2013.4601

758   Fedele, R., & Merenda, M. (2020). An IoT System for Social Distancing and Emergency

759   Management in Smart Cities Using Multi-Sensor Data, 1–24.

760   Gandhimathi, L., & Murugaboopathi, G. (2016). Cross layer intrusion detection and prevention

761   of multiple attacks in Wireless Sensor Network using Mobile agent. In *2016 International*

762   *Conference on Information Communication and Embedded Systems, ICICES 2016* (pp. 1–

763   5). IEEE. https://doi.org/10.1109/ICICES.2016.7518935

764   García-Otero, M., Zahariadis, T., Álvarez, F., Leligou, H., Población-Hernández, A., Karkazis,

765   P., & Casajús-Quirós, F. (2010). Secure Geographic Routing in Ad Hoc and Wireless

766   Sensor Networks. *EURASIP Journal on Wireless Communications and Networking*,

767   *2010*(1), 975607. https://doi.org/10.1155/2010/975607

768   Giri, A., Dutta, S., & Neogy, S. (2020). Information-theoretic approach for secure localization

769   against sybil attack in wireless sensor network. *Journal of Ambient Intelligence and*
770   *Humanized Computing*, (0123456789). https://doi.org/10.1007/s12652-020-02690-9
771   Goyal, S. (2015). Wormhole and Sybil Attack in WSN : A Review. *2015 2nd International*
772   *Conference on Computing for Sustainable Global Development (INDIACom)*, 1463–1468.
773   Retrieved from https://ieeexplore.ieee.org/abstract/document/7100491/
774   Gunturu, R. (2015). Survey of Sybil Attacks in Social Networks. *Scandinavian Journal of*
775   *Surgery*, *98*(1), 25–29. https://doi.org/10.1177/145749690909800105
776   Gupta, B. B., & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural
777   aspects, challenges, and protocols. *Concurrency and Computation: Practice and*
778   *Experience*, (June), e4946. https://doi.org/10.1002/cpe.4946
779   Gupta, D., Bhatt, S., Gupta, M., & Tosun, A. S. (2020). Future Smart Connected Communities to
780   Fight COVID-19 Outbreak, 1–35. Retrieved from http://arxiv.org/abs/2007.10477
781   Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding Security Requirements and
782   Challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and*
783   *Communications*, *2019*. https://doi.org/10.1155/2019/9629381
784   Ishmanov, F., & Bin Zikria, Y. (2017). Trust Mechanisms to Secure Routing in Wireless Sensor
785   Networks: Current State of the Research and Open Research Issues. *Journal of Sensors*,
786   *2017*, 1–16. https://doi.org/10.1155/2017/4724852
787   Jain, U., Hussain, M., & Kakarla, J. (2020). Simple, secure, and lightweight mechanism for
788   mutual authentication of nodes in tiny wireless sensor networks. *International Journal of*
789   *Communication Systems*, *33*(9), 1–16. https://doi.org/10.1002/dac.4384
790   Jamshidi, M., Zangeneh, E., Esnaashari, M., Darwesh, A. M., & Meybodi, M. R. (2019). A
791   Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a
792   Distributed Algorithm to Defend It. *Wireless Personal Communications*, *105*(1), 145–173.
793   https://doi.org/10.1007/s11277-018-6107-5
794   Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015). A sybil attack detection scheme for a
795   centralized clustering-based hierarchical network. *Proceedings - 14th IEEE International*
796   *Conference on Trust, Security and Privacy in Computing and Communications, TrustCom*
797   *2015*, *1*, 318–325. https://doi.org/10.1109/Trustcom.2015.390
798   Jawad, H. M., Nordin, R., & Gharghan, S. K. (2017). Energy-Efficient Wireless Sensor
799   Networks for Precision Agriculture : A Review. https://doi.org/10.3390/s17081781
800   Jinhui, X., Yang, T., Feiyue, Y., Leina, P., Juan, X., & Yao, H. (2018). Intrusion detection
801   system for hybrid DoS attacks using energy trust in wireless sensor networks. *Procedia*
802   *Computer Science*, *131*, 1188–1195. https://doi.org/10.1016/j.procs.2018.04.297
803   John, R., Cherian, J. P., & Kizhakkethottam, J. J. (2015). A survey of techniques to prevent sybil
804   attacks. *Proceedings of the IEEE International Conference on Soft-Computing and Network*
805   *Security, ICSNS 2015*, 1–6. https://doi.org/10.1109/ICSNS.2015.7292385
806   Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and
807   countermeasures. *Proceedings of the First IEEE International Workshop on Sensor*
808   *Network Protocols and Applications, 2003.*, 113–127.
809   https://doi.org/10.1109/SNPA.2003.1203362
810   Khanna, A., & Tomar, R. (2016). IoT based Interactive Shopping Ecosystem. *2016 2nd*
811   *International Conference on Next Generation Computing Technologies (NGCT)*, (October),
812   40–45. https://doi.org/10.1109/NGCT.2016.7877387
813   Kim, J., & Kim, K. (2013). A scalable and robust hierarchical key establishment for mission-
814   critical applications over sensor networks. *Telecommunication Systems*, *52*(2), 1377–1388.

815   https://doi.org/10.1007/s11235-011-9650-x

816   Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009).
817   Systematic literature reviews in software engineering - A systematic literature review.
818   *Information and Software Technology*, *51*(1), 7–15.
819   https://doi.org/10.1016/j.infsof.2008.09.009

820   Kolias, C., Kambourakis, G., & Maragoudakis, M. (2011). Swarm intelligence in intrusion
821   detection: A survey. *Computers and Security*, *30*(8), 625–642.
822   https://doi.org/10.1016/j.cose.2011.08.009

823   Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down
824   survey. *Computer Networks*, *141*, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012

825   Kumari, P., & Sahana, S. K. (2019). An Efficient Swarm-Based Multicast Routing Technique—
826   Review. In H. S. Behera, J. Nayak, B. Naik, & A. Abraham (Eds.) (Vol. 711, pp. 123–134).
827   Singapore: Springer Singapore. https://doi.org/10.1007/978-981-10-8055-5_12

828   Lazos, L., & Poovendran, R. (2005). SeRLoc: Robust Localization for Wireless Sensor
829   Networks. *ACM Transactions on Sensor Networks*, *1*(1), 73–100.
830   https://doi.org/10.1145/1077391.1077395

831   Lazrag, H., Chehri, A., Saadane, R., & Rahmani, M. D. (2020). Efficient and secure routing
832   protocol based on Blockchain approach for wireless sensor networks. *Concurrency*
833   *Computation* , (November), 1–10. https://doi.org/10.1002/cpe.6144

834   Li, Q., & Cheffena, M. (2019). Exploiting Dispersive Power Gain and Delay Spread for Sybil
835   Detection in Industrial WSNs: A Multi-Kernel Approach. *IEEE Transactions on Wireless*
836   *Communications*, *18*(3), 1805–1818. https://doi.org/10.1109/TWC.2019.2897308

837   Liu, G., Wang, X., Li, X., Hao, J., & Feng, Z. (2018). ESRQ: An Efficient Secure Routing
838   Method in Wireless Sensor Networks Based on Q-Learning. *Proceedings - 17th IEEE*
839   *International Conference on Trust, Security and Privacy in Computing and*
840   *Communications and 12th IEEE International Conference on Big Data Science and*
841   *Engineering, Trustcom/BigDataSE 2018*, 149–155.
842   https://doi.org/10.1109/TrustCom/BigDataSE.2018.00032

843   Liu, K., Abu-Ghazaleh, N., & Kang, K. D. (2007). Location verification and trust management
844   for resilient geographic routing. *Journal of Parallel and Distributed Computing*, *67*(2),
845   215–228. https://doi.org/10.1016/j.jpdc.2006.08.001

846   Lu, Y., & Xu, L. Da. (2019). Internet of things (IoT) cybersecurity research: A review of current
847   research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115.
848   https://doi.org/10.1109/JIOT.2018.2869847

849   Luo, Y. (2019). Data Collection Through Mobile Vehicles in Edge Network of Smart City. *IEEE*
850   *Access*, *7*, 168467–168483. https://doi.org/10.1109/ACCESS.2019.2951587

851   Lv, S., Wang, X., Zhao, X., & Zhou, X. (2008). Detecting the Sybil attack cooperatively in
852   wireless sensor networks. *Proceedings - 2008 International Conference on Computational*
853   *Intelligence and Security, CIS 2008*, *1*, 442–446. https://doi.org/10.1109/CIS.2008.69

854   Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y., & Pande, A. (2015). SGOR: Secure and scalable
855   geographic opportunistic routing with received signal strength in WSNs. *Computer*
856   *Communications*, *59*, 37–51. https://doi.org/10.1016/j.comcom.2015.01.003

857   Maddar, H., Kammoun, W., & Youssef, H. (2017). Trust Intrusion Detection System Based on
858   Location for Wireless Sensor Network. In A. M. Madureira, A. Abraham, D. Gamboa, & P.
859   Novais (Eds.) (Vol. 557, pp. 831–840). Cham: Springer International Publishing.
860   https://doi.org/10.1007/978-3-319-53480-0_82

861   Mawgoud, A. A., Taha, M. H. N., & Khalifa, N. E. M. (2020). Security Threats of Social
862   Internet of Things in the Higher Education Environment (Vol. 846, pp. 151–171). Springer
863   International Publishing. https://doi.org/10.1007/978-3-030-24513-9_9
864   Md Zin, S., Badrul Anuar, N., Mat Kiah, M. L. M., & Ahmedy, I. (2015). Survey of secure
865   multipath routing protocols for WSNs. *Journal of Network and Computer Applications*, *55*,
866   123–153. https://doi.org/10.1016/j.jnca.2015.04.018
867   Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE*
868   *Transactions on Emerging Topics in Computing*, *5*(4), 586–602.
869   https://doi.org/10.1109/TETC.2016.2606384
870   Mubarakali, A. (2021). An Efficient Authentication Scheme Using Blockchain Technology for
871   Wireless Sensor Networks. *Wireless Personal Communications*, (0123456789).
872   https://doi.org/10.1007/s11277-021-08212-w
873   Murali, S., & Jamalipour, A. (2020). A Lightweight Intrusion Detection for Sybil Attack under
874   Mobile RPL in the Internet of Things. *IEEE Internet of Things Journal*, *7*(1), 379–388.
875   https://doi.org/10.1109/JIOT.2019.2948149
876   Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The sybil attack in sensor networks, 259.
877   https://doi.org/10.1145/984622.984660
878   Paul, A., Sinha, S., & Pal, S. (2013). An Efficient Method to Detect Sybil Attack using Trust
879   based Model. *Proc. of Int. Conf. on Advances in Computer Science, AETACS An*.
880   Prathusha Laxmi, B., & Chilambuchelvan, A. (2017). GSR: Geographic Secured Routing using
881   SHA-3 algorithm for node and message authentication in wireless sensor networks. *Future*
882   *Generation Computer Systems*, *76*, 98–105. https://doi.org/10.1016/j.future.2017.05.015
883   Prithi, S., & Sumathi, S. (2020). LD2FA-PSO: A novel Learning Dynamic Deterministic Finite
884   Automata with PSO algorithm for secured energy efficient routing in Wireless Sensor
885   Network. *Ad Hoc Networks*, *97*, 102024. https://doi.org/10.1016/j.adhoc.2019.102024
886   Pundir, S., Wazid, M., & Singh, D. P. (2020). Intrusion Detection Protocols in Wireless Sensor
887   Networks Integrated to Internet of Things Deployment : Survey and Future Challenges.
888   *IEEE Access*, *8*, 3343–3363. https://doi.org/10.1109/ACCESS.2019.2962829
889   Qinghua Zhang, Pan Wang, Reeves, D. S., & Peng Ning. (2005). Defending against Sybil
890   Attacks in Sensor Networks, 185–191. https://doi.org/10.1109/icdcsw.2005.57
891   Razacheema, A., Alsmadi, M., & Ikki, S. (2018). Survey of Identity-Based Attacks Detection
892   Techniques in Wireless Networks Using Received Signal Strength. *Canadian Conference*
893   *on Electrical and Computer Engineering*, *2018-May*.
894   https://doi.org/10.1109/CCECE.2018.8447756
895   Razaque, A., & Rizvi, S. S. (2017). Secure Data Aggregation Using Access Control and
896   Authentication for Wireless Sensor Networks. *Computers & Security*.
897   https://doi.org/10.1016/j.cose.2017.07.001
898   Ren, K., Lou, W., Zeng, K., Member, S., Moran, P. J., Sohraby, K., … Znati, T. (2007). *Wireless*
899   *Sensor Networks*. *Booksgooglecom* (Vol. 6). Retrieved from
900   https://dl.acm.org/citation.cfm?id=2480912
901   Roy Chowdhury, A. (2017). IoT and Robotics: a synergy. *PeerJ*, *5*.
902   https://doi.org/10.7287/peerj.preprints.2760
903   Santos, C., Jimenez, J. A., & Espinosa, F. (2019). Effect of Event-Based Sensing on IoT Node
904   Power Efficiency. Case Study: Air Quality Monitoring in Smart Cities. *IEEE Access*, *7*,
905   132577–132586. https://doi.org/10.1109/ACCESS.2019.2941371
906   Sha, K., Gehlot, J., & Greve, R. (2013). Multipath routing techniques in wireless sensor

907   networks: A survey. *Wireless Personal Communications*, *70*(2), 807–829.
908   https://doi.org/10.1007/s11277-012-0723-2
909   Sheron, P. S. F., Sridhar, K. P., Baskar, S., & Shakeel, P. M. (2020). A decentralized scalable
910   security framework for end-to-end authentication of future IoT communication.
911   *Transactions on Emerging Telecommunications Technologies*, *31*(12), 1–12.
912   https://doi.org/10.1002/ett.3815
913   Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2018). A Survey on Sensor-
914   based Threats to Internet-of-Things (IoT) Devices and Applications. Retrieved from
915   http://arxiv.org/abs/1802.02041
916   Ssu, K. F., Wang, W. T., & Chang, W. C. (2009). Detecting Sybil attacks in Wireless SeSsu, K.
917   F., Wang, W. T., & Chang, W. C. (2009). Detecting Sybil attacks in Wireless Sensor
918   Networks using neighboring information. Computer Networks, 53(18), 3042–3056.
919   https://doi.org/10.1016/j.comnet.2009.07.013nsor. *Computer Networks*, *53*(18), 3042–3056.
920   https://doi.org/10.1016/j.comnet.2009.07.013
921   Steiner, R. V., & Lupu, E. (2016). Attestation in Wireless Sensor Networks : A Survey, *49*(3), 1–
922   31.
923   Umar, I. A., Hanapi, Z. M., Sali, A., & Zulkarnain, Z. A. (2017). TruFiX: A Configurable Trust-
924   Based Cross-Layer Protocol for Wireless Sensor Networks. *IEEE Access*, *5*, 2550–2562.
925   https://doi.org/10.1109/ACCESS.2017.2672827
926   Usman, A. B., & Gutierrez, J. (2018). Toward Trust Based Protocols in a Pervasive and Mobile
927   Computing: A Survey. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2018.07.009
928   Vasudeva, A., & Sood, M. (2018a). Survey on sybil attack defense mechanisms in wireless ad
929   hoc networks. *Journal of Network and Computer Applications*, *120*(June), 78–118.
930   https://doi.org/10.1016/j.jnca.2018.07.006
931   Vasudeva, A., & Sood, M. (2018b). Survey on sybil attack defense mechanisms in wireless ad
932   hoc networks. *Journal of Network and Computer Applications*, *120*(June), 78–118.
933   https://doi.org/10.1016/j.jnca.2018.07.006
934   Wang, C., Zhu, L., Gong, L., Zhao, Z., Yang, L., Liu, Z., & Cheng, X. (2018). Accurate sybil
935   attack detection based on fine-grained physical channel information. *Sensors (Switzerland)*,
936   *18*(3), 1–23. https://doi.org/10.3390/s18030878
937   Wang, J., Yang, G., Sun, Y., & Chen, S. (2007). Sybil attack detection based on RSSI for
938   wireless sensor network. *2007 International Conference on Wireless Communications,*
939   *Networking and Mobile Computing, WiCOM 2007*, (06), 2684–2687.
940   https://doi.org/10.1109/WICOM.2007.667
941   Wen, M., Li, H., Zheng, Y., & Chen, K. (2008). TDOA-based Sybil attack detection scheme for
942   wireless sensor networks. *Journal of Shanghai University (English Edition)*, *12*(1), 66–70.
943   https://doi.org/10.1007/s11741-008-0113-2
944   Wu, Z., & Ma, R. (2019). A Novel Sybil Attack Detection Scheme Based on Edge Computing
945   for Mobile IoT Environment. Retrieved from http://arxiv.org/abs/1911.03129
946   Yuan, Y., Huo, L., Wang, Z., & Hogrefe, D. (2018). Secure APIT Localization Scheme Against
947   Sybil Attacks in Distributed Wireless Sensor Networks. *IEEE Access*, *6*, 27629–27636.
948   https://doi.org/10.1109/ACCESS.2018.2836898
949   Zeb, A., Islam, A. K. M. M., Zareei, M., Mamoon, I. Al, & Mansoor, N. (2016). Clustering
950   Analysis in Wireless Sensor Networks : An ambit of Performance Metrics and Schemes
951   Taxonomy, 1–48.
952   Zhan, G., Shi, W., & Deng, J. (2012). Design and implementation of TARF: A trust-aware

953   routing framework for WSNs. *IEEE Transactions on Dependable and Secure Computing*,
954   *9*(2), 184–197. https://doi.org/10.1109/TDSC.2011.58
955 Zhang, Q., & Zhou, X. (2010). Efficient distributed location verification in wireless sensor
956   networks. *Frontiers of Computer Science in China*, *4*(1), 123–134.
957   https://doi.org/10.1007/s11704-009-0071-x
958 Zhong, S., Li, L., Liu, Y. G., & Yang, Y. R. (2004). Privacy-preserving locationbased services
959   for mobile users in wireless networks. *Yale Computer Science, Tech. Rep. YALEU/DCS/TR-*
960   *1297*, 1–13. Retrieved from
961   http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Privacy-
962   Preserving+Location-based+Services+for+Mobile+Users+in+Wireless+Networks#0
963 Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J., & Teo, J. C. M. (2015). Toward energy-
964   efficient trust system through watchdog optimization for WSNs. *IEEE Transactions on*
965   *Information Forensics and Security*, *10*(3), 613–625.
966   https://doi.org/10.1109/TIFS.2015.2389145
967 Zhu, M., Chang, L., Wang, N., & You, I. (2020). A smart collaborative routing protocol for
968   delay sensitive applications in industrial IoT. *IEEE Access*, *8*, 20413–20427.
969   https://doi.org/10.1109/ACCESS.2019.2963723
970 Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale
971   distributed sensor networks. *ACM Transactions on Sensor Networks*, *2*(4), 500–528.
972   https://doi.org/10.1145/1218556.1218559
973 Zhuang, T., Ren, M., Gao, X., Dong, M., Huang, W., & Zhang, C. (2019). Insulation Condition
974   Monitoring in Distribution Power Grid via IoT-Based Sensing Network, *34*(4), 1706–1714.
975

Existing literature review on Sybil Attack countermeasures

Reference	Key management	Resource Testing	Encryption	Trust	RSSI	Watchdog	TDOA	Metahueristic	Incentive based	Application Domain
This paper	✓	✓	✓	✓	✓	✓	✓	✓	X	WSN
(Vasudeva & Sood, 2018)	✓	✓	✓	✓	✓	✓	✓	X	X	WANET
(Bhise & Kamble, 2016)	✓	✓	X	X	✓	X	X	X	✓	Social Network & WSN
(Gunturu, 2015)	✓	✓	X	✓	X	X	X	X	X	Social Network

Research Questions

RQ#	Research questions	Motivations
RQ1	What is Sybil and Blackhole Attack?	These two questions will prove the aim of countermeasure for Sybil and Blackhole attack
RQ2	Why is it to focus on these two attacks in WSN and IoT environment?	These two questions prove the purpose of countermeasure for Sybil and Blackhole attack
RQ3	Where will new researchers concentrate on creating a new method?	This question is intended to help researchers look deeper into the research issue
RQ4	How can the countermeasures in the Sybil and Blackhole attain better algorithms to thwart these attacks?	This question is intended to explain countermeasure use to thwart Sybil and Blackhole attack in obtaining optimal algorithms, identifying challenges and techniques.

Sybil attack countermeasures comparison

Author, Year	Advantages	Disadvantages	Countermeasure Method	Type of Countermeasure			IoT Ready	Simulator
				Prevention	Detection	Mitigation		
García-Otero et al. (2010)	Energy efficient	Communication overhead	Trust		✓			AWISSENET test-bed.
Zhang et al. (2010)	low false positive rates at the same time even with high location inaccuracy	High communication overhead due to exchange of trust information	Encryption and Trust	✓	✓		✓	Mathematical proof
Claycomb, et al. (2011)	A new approach to key establishment, which combines a group-based distribution model and identity-based cryptography	High complexity	Encryption	✓				NA
He et al.(2011)	EDDK utilizes encryption method is more advantageous in computation, communication, and storage	High computation	Encryption	✓				MATLAB
Dong et al. (2012)	Extend the lifetime of the whole network.	Does not support dynamic regular sensor node addition after initial deployment	Encryption	✓				TelosB motes
Zhan et al. (2012)	TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment	TARF is suitable only for static environment	Trust		✓		✓	MATLAB
Kim et al. (2013)	Less storage, computation and communication cost	High processing	Encryption	✓				Mathematical proof
Lyu et al. (2015)	Lightweight and distributed	High communication	Trust & RSSI	✓	✓		✓	OPNET

Reference	Advantage	Disadvantage	Method						Tool
			load						
Sarigiannidis et al. (2015)	Lightweight and distributed	Mobility is not considered and not energy efficient	Using UWB antenna dan revoke malicious when detected			✓	✓		MATLAB
Zhou et al. (2015)	Lightweight and energy efficient	High communication overhead	Watchdog using Trust			✓			WSNET
Jan et al. (2015)	Improve network lifetime	The system fails if a malicious node able to imitate high energy node	RSSI			✓		✓	NA
Saleem et al. (2016)	Provide security through encryption with minimum processing time	Artificial immune system (AIS) - he major limitation of BIOSARP is that it requires time to develop the knowledge of the overall network during the initialization decryption - computational overhead	Encryption	✓				✓	NS2
Alsaedi et al. (2017)	Lightweight and able to detect Sybil nodes accurately	Higher memory requirement	Energy trust calculation			✓		✓	OMNeT++
Prathusha et al. (2017)	Higher security due to the encryption method	Higher processing resources	Encryption	✓				✓	NetTopo
Raja et al. (2017)	Higher security due to the encryption method	Higher processing resources	Encryption using Fujisaki Okamoto Algorithm	✓					NS2
Maddar et al. (2017)	Lightweight	High communication overload	Trust calculation			✓			MATLAB
Razaque et al. (2017)	Higher security due to the encryption method	Higher processing resources	Encryption	✓					NS3
Yuan et al. (2018)	Lightweight	Not reliable due to radio interference	Localization with RSS signal			✓			MATLAB

		and signal propagation						
Wang et al. (2018)	Sybil attack detection system achieves high accuracy for both static and dynamic scenarios using CSI	It is not easily obtainable on the shelf NICs	CSI & RSSI		✓			MATLAB
Jamshidi et al. (2019)	Lightweight	Not reliable due to radio interference and signal propagation	RSSI	✓	✓		✓	J-SIM
Li et al. (2019)	Higher accuracy and able to detect Sybil node	High processing load and communication overhead	Channel feature in terms of power gain and delay spread.		✓			MATLAB
Liu et al. (2020)	Rapid localization capability and high precision detection with low energy consumption.	Not reliable due to radio interference and signal propagation	RSSI		✓		✓	-
Angappan et al. (2020)	Can apply to any resource-constrained WSN	It takes up memory if the device has limited	RSSI		✓		✓	NS2
Prithi et al. (2020)	Better throughput and network lifetime	PSO easily to fall into local optimum and low convergence rate in the iterative process. ..	Learning Dynamic Deterministic Finite Automata		✓			MATLAB
Jain, Hussain et al. (2020)	Hence, the proposed mechanism is best suitable for resource constraint nodes	Hierarchical network topology suffers from non-uniform clustering, high energy dissipation, and less lifespan of the sensor nod	Authentication	✓				AVISPA and Scyther tools

Giri et al (2020)	Successfully detect sybil attack and increase localization accuracy despite sybil attack.	High processing requirement	Localization with RSS signal		✓			na
Raghav et al. (2020)	Beeware based secure and optimized routing scheme with the help of bee algorithms.	High processing requirement & moderate scalability Its disadvantages include the diversity of race is poor. When the solution is close to the global optimum, it is easy to fall into the local optimum, resulting in a stagnation phenomenon	Encryption & Bee Algorithm	✓			✓	MATLAB
Bhushan et al. (2020)	Enhances energy efficiency and makes the network secure	Does not cover for availability	Trust and ACO		✓			NA

Figure 1

The selection of process of articles in the form of diagram
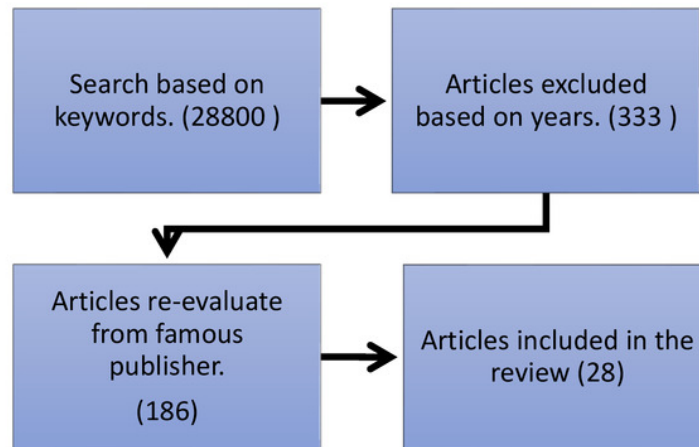
Figure 2

The classification of Attack in WSN and IoT
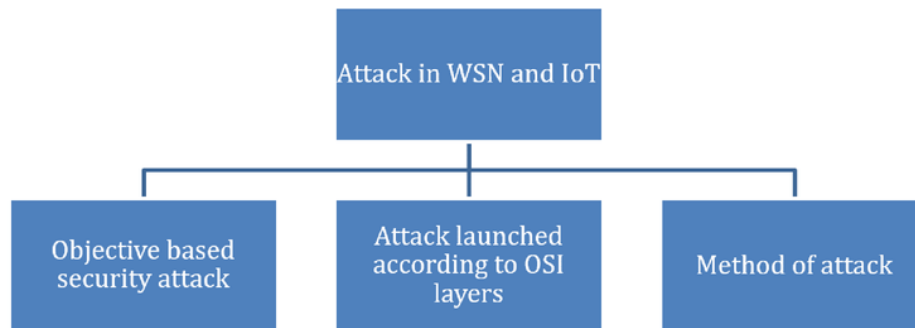
Figure 3

Sybil attack countermeasures framework
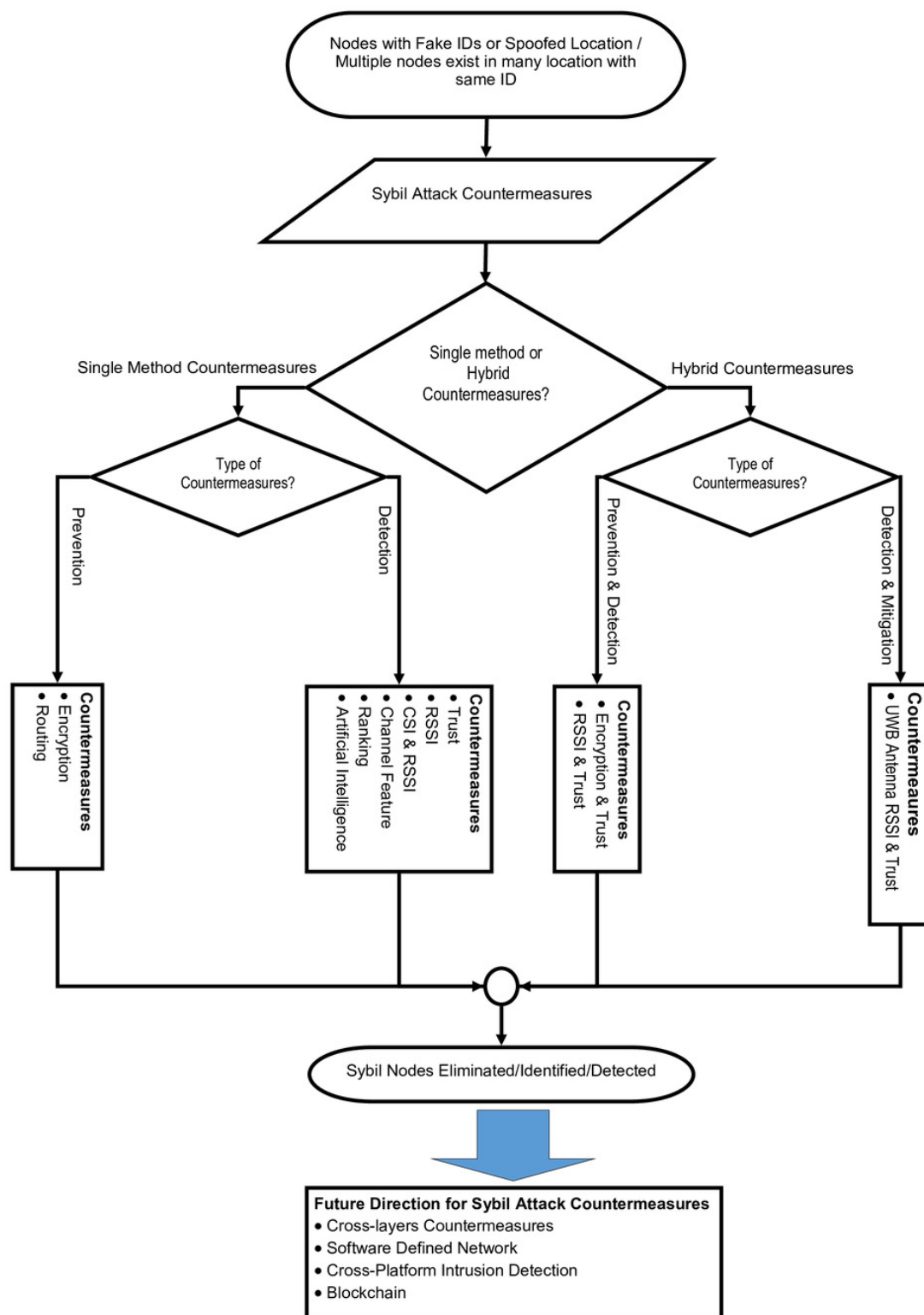
Figure 4

The Sybil attack in geographic routing
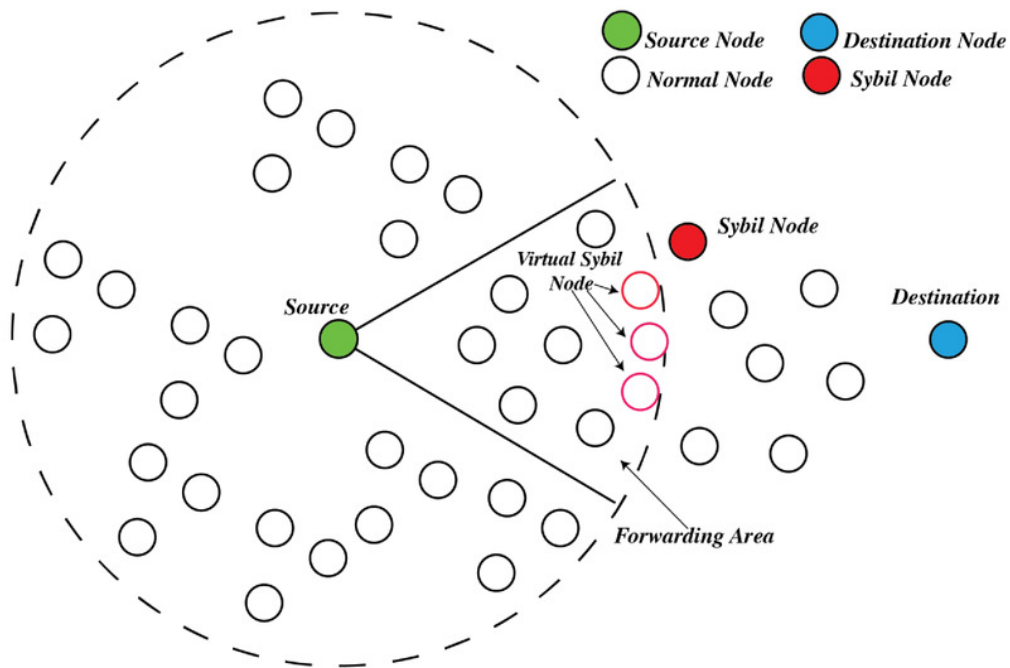
Figure 5

Distribution of the Sybil attack countermeasures between 2010 and 2010
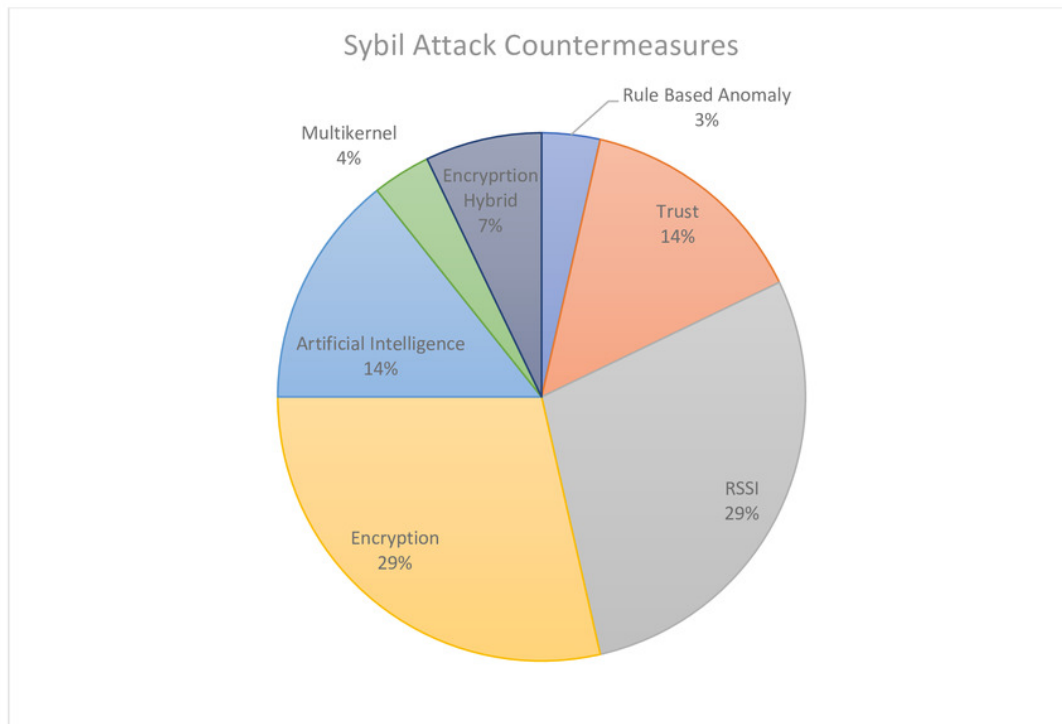
Figure 6

Number of papers on Sybil Countermeasures between 2010 and 2020