Crypto Hash Signature Adopted Blockchain to Detect Spiteful Node to Enhance the Throughput in WSN

Ambika Bhuvaneswari Ca and E D Kanmani Ruby a
a Electronics & Communication Engineering Department, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, 600062.
ambika.bhuvaneswari@gmail.com, dredkanmaniruby@veltech.edu.in

Article Info
Page Number: 76 – 84
Publication Issue:
Vol. 71 No. 3s (2022)

Abstract
Secured routing is the definite maneuvers in a wireless sensor network (WSN) for distributing data packets to the base station. However, attacker node outbreaks will occur throughout the routing process, exacerbating the wireless sensor network's functioning. As a result, a secure routing protocol is essential to ensure route fortification and the effectiveness of wireless sensor networks. For this reason, many studies have shown an interest in improving routing protocol security by adopting cryptographic structures and trust regulation methods. However, most secured routing protocols are dynamically awful in real-time scenarios, making it difficult to distinguish between unsecured routing node performances. In the same way, solutions for detecting and mitigating node attacks are still challenging. In this, Crypto Hash signature (CHS) token are generated for the flow accesses with a secret key belonging to each routing sensor node. The assessment metrics corresponding to average energy consumption, and throughput of token transactions is measured. Then the simulation performance of the proposed SDOR-CHS-SD method provide 18.46%, 8.37% and 26.77% higher token transactions throughput, when compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively.

Keywords: WSN; Crypto Hash Signature; Hash Function; Block Chain: Throughput; Packet Delay;

Article History
Article Received: *22 April 2022*
Revised: *10 May 2022*
Accepted: *15 June 2022*
Publication: *19 July 2022*

1. Introduction

The sensor networks will become pervasive in the future to improve future technology, the environment, and infrastructure. Health care, smart houses with sensors, environmental monitoring, and other applications are among them. A gateway is used to communicate data in a WSN. Because hostile communications can be intercepted, erased, or misdirected, confidentiality, message veracity, and authentication are critical circumstances. As a response, appropriate communication channel security solutions should be deployed.

In [1,2] because of resource constraints, Hardware manipulation, eavesdropping, and misleading message insertion, among other security issues, are all possible with wireless

sensor structures. As a result, the network receives more effective security methods that comply to particular WSN features. The most common security technique that can provide security characteristics is synchronous cryptography. In such security approaches, while two nodes want to interact with one another, they use a public key encryption and decryption procedures. The nodes have previously chosen and shared this symmetric key to offer information sanctuary and validation. The technique of creating shared symmetric keys is known as key management. In both unsupervised and supervised systems, there is indication that using nodes are put at risk when they use these symmetric designed for various sessions. Despite the existence of tools for maintaining and restoring network nodes, there are always attacks that must be discovered and countered.

2. Related Works

In, [3] the author presented a dynamic validation technique built on the hash function for protecting sensor networks. In, [4] presented another approach based on two-factor authentication that is highly efficient in the same period. The techniques are vulnerable to man-in-the-middle attacks, is proposed in [5] offered the RSA-based authentication mechanism. Due to the protocol's public key holding of sensor nodes and users, the suggested approach required a large storage capacity. He et al. [7] offered a protected wireless sensor network, a temporal-credential built mutual authentication and key agreement method with virtual individuality is proposed. whereas the author in [6] presented a certification and key arrangement protocol for heterogeneous ad hoc WSN. In, [8] obtain a smart card authentication system for a disseminated cloud environment construction in 2016. The enumerated users can access private data from all private cloud servers in a secure manner under this arrangement. They also stated that Turkanovic et al protocol's [6] had two types of security issues, and they have the capability to mitigate these flaws. The author, [9] employing a three-factor user authentication approach, offered a resourceful dynamic and factors relevant system for hierarchical wireless sensor networks. Founded on the hyper elliptic curve [10] suggested a lightweight numerous shared key agreement for wireless sensor networks. The approach diminishes key argument overhead while also growing key security. In [11] the author suggested a trivial password authentic key argument for heterogeneous wireless sensor networks. They looked into three freshly suggested 3-PAKE protocols and labelled their flaws. Their unique 3-PAKE protocol delivers provably secure, adaptable, and efficient security features.

3. Proposed Work:

Network Deployment: In the presented design approach, 300 nodes are distributed in the network, with a base station at the middle. Cluster heads (CHs) are picked depending on their capacities, while the remainder are regarded nodes of normal in character. Furthermore, blockchain is applied on the CHs and base station because they have large data storage and processing resources. By keeping a record of every transaction in its ledger, the private blockchain is coupled with sensor nodes to protect the network and data's security. Furthermore, the nodes are recorded in the blockchain, and each node is assigned a unique

number. Furthermore, because the consensus of PoA is for the private block chain technique, and the transaction has been validated.

3.1 Registration and Authentication:

Since the nodes are placed in a hostile, unmanaged location, authentication is required. In this scenario, attackers may target nodes in addition to nodes. These hackers gain physical contact to certain nodes and exploit their network connections. In addition, attackers can exploit the node IDs to re-enter the network and perform other unethical acts. As a result, several writers have proposed various blockchain-based registration and authentication procedures, where the possibilities of nodes acting maliciously are minimal due to blockchain's unique qualities, as has already been mentioned.

Although hashes are recorded on the blockchain in most documents, which may be guessed by various techniques such as brute force assault and are used in malicious activities, there are still chances of various sorts of attacks that can be carried out by altering its identities of nodes in the network. As a result, a secure registration and authentication system is presented in this section. However, when compared to standard storage methods, blockchain storage is extremely expensive. As a result, the registration and authentication processes have been simplified to reduce the storage burden imposed by blockchain. The system will be less benefited, according to our network's requirements, because nodes have a restricted time period for communication.

3.2 Crypto hash Function:

Crypto hash functions are a type of cryptography that ensures data integrity. A block cipher takes varied-length of input and returns a hash value with a set length. It's frequently used in security systems such as digital signatures and Message Authentication Codes [16]. In Fig.1 the digital signature for node authentication and verification has been illustrated.

The National Bureau of Standards originally employed the simple XOR applied to 64-bit blocks of the message and then the encryption of the complete message as block cyphers as hash functions for Hash functions. Consider dividing the message sequence into 64-bit blocks of fixed size x_1, x_2, x_3,.....x_n, and defining the hash code C as the XOR representation of each individual blocks of all blocks. The final block code is nothing but appending of all hash code.

$C = a_{n+1} = a_1 \oplus a_2 \oplus \ldots\ldots \oplus a_n$

$h_i = EX_i(H_{i-1})$

$G = h_n$

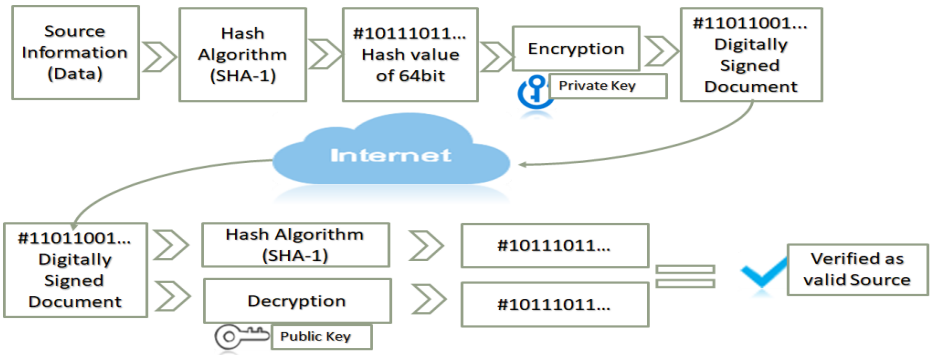

Figure. 1: Digital Signature to authenticate the node

Collision resistance, speed, input and output block length are the most important aspects of a cryptographic hash function. 1) Hash Algorithm with a Secure Hash, The National Institute of Standards and Technology (NIST) [17] has issued a family of cryptographic hash functions called Secure Hash Algorithms.

In this part, the Secure Hash algorithm (SHA-1) is used to create a Crypto Hash Signature Token for wireless sensor networks, which is used to protect the wireless sensor networks' decentralised database. Crypto Hash Signature (CHS) tokens are created for flow accesses using a secret key belonging to each routing sensor node, and it also provides the best data transmission method. The hash function is a mathematical function that determines the length of numerical data based on its randomness and then converts it to fixed length numerical data. The input can be any length (smaller or greater), but the output will always be the same size. If the same input is utilised numerous times, the hash value generated is always the same. Conversely, if the data collected (text) is altered, the hash value is immediately modified in a different manner. The original input cannot then be derived from the hash value. That is to say, the opposite is not possible. Because the reverse operation is impossible, the hash function is not encryption. The Crypto Hash Signature takes the input and generates the hash value, which is formatted as follows:

SHA -1 hash value:

0 x 5cd9db2120b5c96839c59a87b9ed5e878fb36f790b04d031bfdc2da5bd61aac3

Generally, the crypto hash technique is done based on the following equation (1)

SHA-1 Fun(Trans)=Op Gen. (1)

Then the public key is generated is based on the following equation (2)

$PK= KeyGen^{Trans}|(prime\ number)|$ (2)

For two different transactions that produce the same hash value, the dispute confrontation is implemented using crypto hash algorithms. When the identical hash value is achieved for two transactions, this is referred to as a brute force attack, as shown below (3)

Hash (Trans1) = Hash (Trans2) (3)

In contrast, instead of saving the passwords, the sensor node endorsement validates the sensor node register. Then, prior to database storage, it submits during the Crypto Hash Signature function. The sensor node confirmation is then based on this finding. The node registration and authentication of sensing node from that the identification and prevention of spiteful node is explained in the following algorithm.

3.3 Spiteful Node identification:

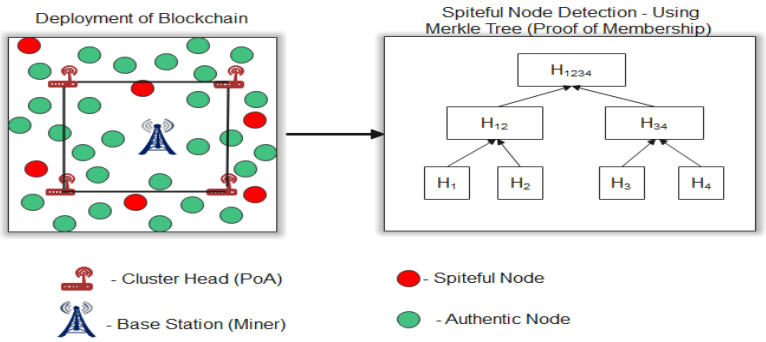

Figure 2: Spiteful Node Detection Using Merkle Tree

In logarithmic time and space, a sorted Merkle tree can also be used to demonstrate non-membership is shown in Figure 2. That is, it is possible to demonstrate that a certain transaction is not part of the Merkle tree. This can be accomplished by presenting a path to the transaction that comes before and after the one in question. If these two components in the tree are sequential, it proves that the item in question is not included, because if it were, it would have to fit between the two things presented, which it doesn't because they are sequential.

Algorithm: Node Authentication

Sn: Sink Node; No: No. of sensor node; G: Hash value; CH: Cluster Heads;
Mi : information msg; Mq: Message Query; Ap: Approval; A: Authorization; Nw: Network; DP:Pkts; DC: Distance of clusters; Ti: Time to broadcast; Vs : Verified sensor node; Gn: genuine node; Pn : prohibited node;
En: network deployment.

1. Initialize Mi, Nid, No, Ti, DC
2. Result (A, G)
3. In the access control model, for every member, do
4. All member sensor clusters get a query message from CH (Mq)
5. The sensor nodes compute, after receiving (Mq).
6. Mq = (CHid kNw id kMikT)
7. CH → Mq
8. If fangled node joins in network
9. No in En ∈ Nw
10. CH notify Nw
11. Nw recall N
12. Nw explore G (Nid, No, Ti, DC) for Vs
13. set A for N; A = (T, DC, Nid, Sn, Mi, DP)
14. Sn patterned broadcast A(Mq) with CH
15. If N== Vs = Gn(N) and
16. N== Mq then , Bs permitted N == Vs belongs to Sn
17. Else
18. N not equal to Vs and N not equal to Mq Pn = Vs
19. Sn not equal to N and prohibited to Nw
20. end
21. end
22. end

4. Simulation results and Discussion:

The scenarios were simulated to ensure that the suggested system model performs as expected. Metamask, Ganache, and Remix-IDE are simulation environments used in the proposed work for blockchain implementation. Furthermore, for interface blockchain with networks, Python-based Web3.api are employed.

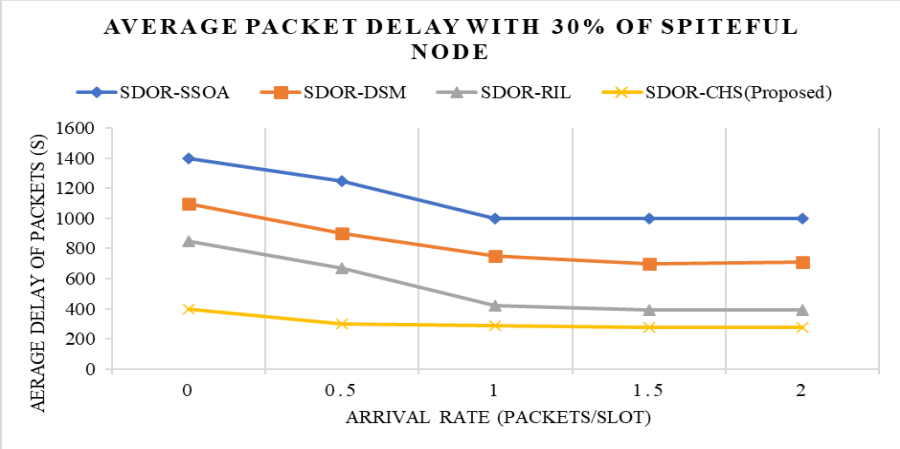

Figure 2: Performance of average packet delay with 30% spiteful node

Figure 2 depicts the performance of average packet delivery delay performance with 30% spiteful node. At arrival rate 0, the proposed SDOR-CHS method provides 54.76%, 55.33% and 33.25% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 0.5, the proposed SDOR-CHS method provides 11.03%, 22.06% and 10.02% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 1, the proposed SDOR-SA-GACN-FSA-CHS-BWSN method provides 41.03%, 32.06% and 11.02% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 1.5, the proposed SDOR-CHS method provides 32.10%, 33.12%, and 21.02% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 2, the proposed SDOR-CHS method provides 21.08%, 6.07%, and 11.95% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively.

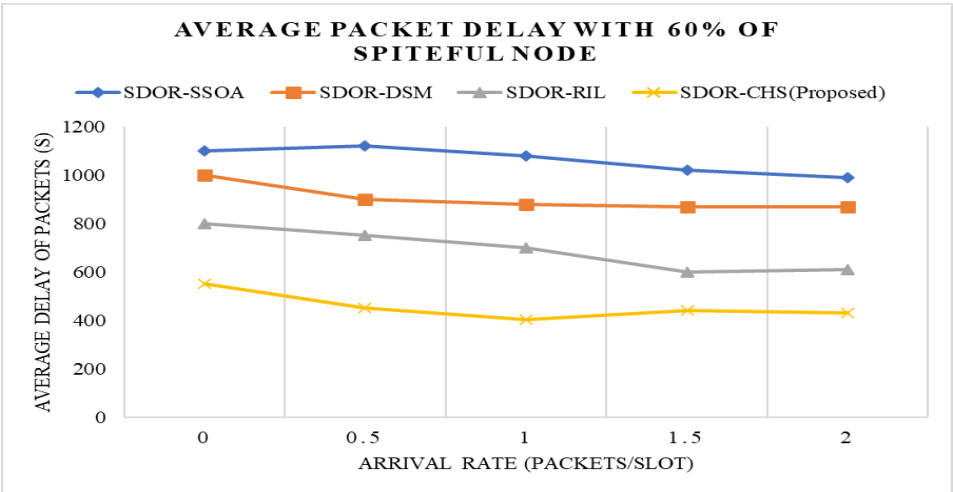

Figure 3: Performance of average packet delay with 60% spiteful node

Figure 3 depicts the average packet delivery delay performance with 60% spiteful node. At arrival rate 0, the proposed SDOR-CHS method provides 69.67%, 53% and 32.87% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 0.5, the proposed SDOR-CHS method provides 12.11%, 25.33% and 32.5% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 1, the proposed SDOR-CHS method provides 38.97%, 38.97% and 33.12% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 1.5, the proposed SDOR-CHS method provides 38.97%, 40.12% and 28.17% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At arrival rate 2, the proposed SDOR-CHS method provides 53.86%, 42.56% and 32.86% lower average delay of packets compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively.

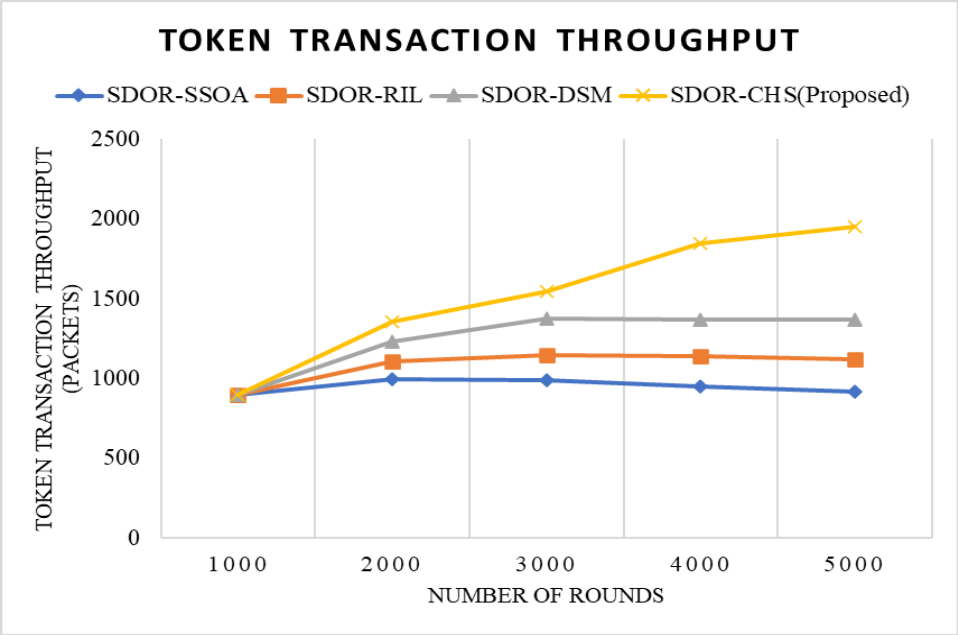

Figure 4: Average token transaction throughput performance

Figure 4 shows the Average transaction throughput performance of block chain system. At concurrent request rate 1000s, the proposed SDOR-CHS method provides 42.5%, 17.61% and 48.45% higher throughput compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At concurrent request rate 2000s, the proposed SDOR-CHS method provides 38.75%, 43.86%, and 37.86% higher throughput compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At concurrent request rate 3000s, the proposed SDOR-CHS method provides 37.86%, 12.32% and 43.76% higher throughput compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At concurrent request rate 4000s, the proposed SDOR-CHS method provides 36.86%, 45.75% and 39.75% higher throughput compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively. At concurrent request rate 5000s, the proposed SDOR-CHS method provides 53.75%, 48.97%, and 35.86% higher throughput

compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively.

5. Conclusion:

Crypto Hash Signature adopted blockchain to detect spiteful node is successfully implemented for the improvement of throughput in WSNs. The secured routing to improve the throughput analysed using identifying and preventing the spiteful node. Here the proposed cryptographic blockchain wireless network based on the view point of proof of authority consensus procedure, average packet delay with spiteful nodes and average token transaction for throughput have been analysed. From that proposed method is 18.46%, 8.37% and 26.77% higher token transactions throughput, when compared with existing method like SDOR-SSOA, SDOR-DSM and SDOR-RIL respectively.

References

[1] C. A. Bhuvaneswari and G. Vairavel, "Optimized energy using centralized clustering protocol in heterogeneous wireless sensor networks," ARPN Journal of Engineering and Applied Sciences, vol. 16, no. 2, pp. 215–223, 2021.

[2] C. A. Bhuvaneswari and E. D. K. Ruby, "HETA: end-to-end delay analysis of enhanced centralized clustering protocol for wireless sensor networks," International Journal of System Assurance Engineering and Management, vol. 11, 2021.

[3] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, ''A dynamic user authentication scheme for wireless sensor networks,'' in Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput. (SUTC), vol. 1, Jun. 2006, p. 8.

[4] M. L. Das, ''Two-factor user authentication in wireless sensor networks,'' IEEE Trans. Wireless Commun., vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[5] R. Song, ''Advanced smart card-based password authentication protocol,'' Comput. Standards Interfaces, vol. 32, nos. 5–6, pp. 321–325, Oct. 2010.

[6] M. Turkanović, B. Brumen, and M. Hölbl, ''A novel user authentication and key agreement scheme for heterogeneous ad hoc w+698-86+ireless sensor networks, based on the Internet of Things notion,'' Ad Hoc Netw., vol. 20, pp. 96–112, Sep. 2014.

[7] D. He, N. Kumar, and N. Chilamkurti, ''A secure temporal-credential based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks,'' Inf. Sci., vol. 321, pp. 263–277, Nov. 2015.

[8] R. Amin and G. P. Biswas, ''A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,'' Ad Hoc Netw., vol. 36, pp. 58–80, Jan. 2016.

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

[10] V. S. Naresh, S. Reddi, and N. V. Murthy, ''Provable secure lightweight multiple shared key agreement based on hyper elliptic curve Diffie–Hellman for wireless sensor networks,'' Inf. Secur. J., Global Perspective, vol. 29, no. 1, pp. 1–13, 2020.

[11] I. Santos-González, A. Rivero-García, M. Burmester, J. Munilla, and P. Caballero-Gil, ‘‘Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks,’’ Inf. Syst., vol. 88, Feb. 2020, Art. no. 101423.

[12] PhD Madhusudan Singh, "Blockchain-Based Secure Decentralized Vehicle communication," IEEE, Songdo, South Korea, 2017.

[13] R. Martin, "10 Applications for Blockchain in Connected Car Automotive," ignite, 29 November 2018. [Online]. Available: https://igniteoutsourcing.com/Blockchain/Blockchain automotive-industry/. [Accessed 16 6 2019].