Analytical Model for Evaluating Key Strength Probability in Wireless Sensor Networks

1Turki Alshammari, 2Mohammed Alwakeel
1Researcher, 2Professor
1Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia

Abstract - **The applicability of wireless sensor networks (WSN) to a wide spectrum of applications has been largely proved. However, the risk of a seizure of the network as well as data transferred via it is always attached to the use of WSN, which marks the need for safety measures to impede spoofing. Encryption with the use of cryptography algorithms is the most frequent means of ensuring the security of the network and privacy of the data transmitted. The uniqueness of our system lies in the assistance provided to the user for deciding on a security protocol so that our WSN can ensure the minimum degree of security that is needed. In addition, our system determines the duration of security of a private key in a node which does not need to start with the mechanism of key exchange, as it poses an enormous load on a size-restricted resource node. This research assists in building an analytical framework to evaluate the performance of numerous algorithms of cryptography employed in WSN. This assessment particularly uses an indispensable strength probability measure. The designed algorithm is adequately adaptable and easily applicable to compare the performance of various algorithms. The created system is anticipated to furnish the desirable QoS to WSN and conserve the member node's energy.**

keywords - **Cryptography Algorithms, Wireless Sensor Network, Security Metrics, Key Strength Probability.**

I. INTRODUCTION

The formation of a Wireless Sensor Network (WSN) usually entails a connection between multiple small-sized sensor nodes [1-3]. WSN processes the inputs collected from the ambiance, such as sound, light, vibration, temperature, pressure, and such factors [4]. The major importance allies with the management of the finite resources of these nodes, especially batteries, so that the nodes can continue operating for a prolonged period of time. This approach is distinguished by choosing an optimal safety mechanism for a specific WSN that offers an admissible degree of safety with the use of minimal sensor node resources.

Cryptography has long been employed for ensuring WSN security in its variable functionalities, including environmental monitoring, home automation, climate variation, and traffic supervision. The availability, authentication, confidentiality, and integrity contribute to the core safety requirements of a wireless sensor network [5]. Confidentiality implies that the information extracted from any sensor grid is filtered from an attacker and kept intact and private inside the network. Additionally, the readings of the sensor nodes are inaccessible to their abuts, barring the ones who are permitted for the same, thus creating the need for a resilient primary distribution technique. Prevention of possible traffic investigation strikes requires public data like public keys and sensor IDs to be encrypted in certain cases. The authentication ensures the reliability of a sender via the determination of its origin. Integrity assures that a message received on the network is neither tampered with nor misinterpreted or altered. Lastly, availability ensures the presence of wireless sensor network resources and services at all times.

The relatively restricted limit of resources like communication, power, and processing ability makes the selection of a suitable cryptography mechanism critical to a wireless sensor network. The approaches of cryptography are classified into three major categories, namely symmetrical, asymmetrical and hybrid [5].

A distinctive covert key is jointly used for encryption and decryption at the end of both sender and receiver under symmetrical cryptography. Two popularly recognized algorithms of symmetrical cryptography are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Low consumption of energy in symmetrical mechanisms sometimes makes them preferable over asymmetrical approaches in wireless sensor networks. In around 1974, a team of IBM created DES, which was later sanctioned by the National Institute of Standards and Technology (NIST) to be finally embraced as a national standard in 1997 [6]. It involves a symmetrical key block decoder having a block of 64-bit size and a 56-bit long key. DES has been further enhanced by AES, which is quicker and more versatile with a large number of additional platforms [6]. It may also be used with changeable key lengths of 128, 192, and 256 bits.

On the contrary, asymmetrical cryptography involves the usage of a pair of private and public keys rather than an individual shared key. The public key can be accessed by everyone for encryption of messages, whereas the private key is held secretly by the owners to be used for deciphering and reading the message, as represented in Figure 1. Rivest-Shamir-Adleman (RSA) algorithm exemplifies an extensively used asymmetrical approach [7]. The strength of encryption in the case of RSA is based on the size of the key and doubling or tripling the size of the key augments the strength of coding exponentially [8,9].

The hybrid technique involves the combined usage of both symmetrical and asymmetrical encryption techniques to fetch the benefits of both approaches. SSH and TLS protocol are common examples of hybrid techniques wherein pairing of public and private keys (asymmetric cryptography like Diffie-Hellman) is employed under the mechanism of exchanging keys, and sharing key mechanism (symmetric cryptography like AES) is engaged for transmitting data. Other similar examples include OpenPGP file format and PKCS #7 (reference ad RFC 2315 and RFC 4880).

The performance of encryption mechanisms in the WSN is assessed by using three key matrices termed safety, efficiency, and adaptability [10].

Security Metrics

Multiple safety criteria can be used in this metric for assessing the performance of required algorithms, for example:

Node Validation: The validation of the identity of sender and receiver nodes should be ensured by the key management system.

Resilience: This implies the reaction of a safety mechanism against physical attacks on the node, wherein the information is captured physically from the memory of the sensors.

Node Cancellation: This corresponds to the dynamic ability of the system to discover and revoke the compromised nodes from the network.

Efficiency Metrics

The efficiency metrics of this algorithm include:

Resource Utilization: The extent to which memory, bandwidth, processing and energy are required for key management.

Key Connectivity: Implies the possibility of establishment of shared keys by the (groups of) sensor nodes.

Flexibility Metrics

The flexibility metrics of algorithms include:

Degree of knowledge of the previous usage: Reliability of managing and sharing keys on their position in the network.

Scalability: The potential of adding new nodes to the network without compromising with safety.

II. Related Work

Data protection of WNS is a crucial matter and has been a majorly prioritized research topic as the rapid emergence of advanced tools and technologies creates the need for updating security protocols in conjunction with new threats. Few popular algorithms have been proposed by [4,5,11-14]. The research authors [4] has crafted an intrusion detection system using the neighboring detection approach to identify selective transportation, jamming, and flood crises. The system was intended to execute the Collection Tree Protocol on the TinyOS system (CTP). The researcher's statements based on the achieved results accord precision to the neighbor-based detection method, especially in the presence of excellent collaboration between adjacent nodes. Article [12] studies, analyses, and compares multiple cryptographic models. Study [12] showed a dynamic key update method in a symmetrical security plan that was set up on a trustworthy node termed as a leading node or trusted third party. The TOSSIM simulation software in the operating system of TinyOS analyzed WSN's encryption method for memory use, energy, and time criteria [11]. The architecture of the IoT network and issues linked with its security are explained in the article [13] that analyses the major studies on the safety and confidentiality of data in Wireless Sensor Networks (WSNs). Later, they suggested an effective algorithm for a media-based monitoring system in the IoT network for smart cities, which integrates two techniques for WSN packet routing and safety presented by previous researchers. Simultaneously, it also recuperates the new compression specification for media, namely High-Efficiency Video Coding (HEVC). The efficiency of the recommended model linked with media security, users' privacy, and memory requirements of sensor nodes can be illustrated in experimental studies. We focus largely on safety measures used to assess the effectiveness of encryption methods. Few recent propositions of fundamental management solutions of WSN have been analyzed in a research study [10] and examined on the basis of safety measures. A Sensor Data Security Estimator (SDSE) was proposed for WSN [15], which is a safety metric used for predicting the security level of sensor data on the basis of analysis of detection techniques as well as attack prevention.

III. Proposed analytical model to evaluate key strength probability in wireless sensor networks

Given that various encryption algorithms may be employed in sensor networks, and considering the restricted resources in similar networks, it is necessary for a network administrator to develop a mechanism to pick the algorithms displaying optimal performance on the basis of resources available in the network. Research analysts have proposed multiple techniques for contrasting the performances of encryption algorithms employed in sensor networks. Most of these approaches demand the implementation of the chosen algorithm in a real setting use of a costly simulation framework to identify the network's optimal algorithm. Thus, it becomes easier for the network management to pick the right algorithm at the lowest effort and expense with a simple and cost-effective approach to measure the performance of cryptographic algorithms.

This paper presents an analytical framework to contrast the performance of multiple encryption algorithms on the basis of Key Strength Probability (KSP). There is a likelihood that a node's private key remains safe and undiscovered by a forceful barbarian seizure. If the possibility is greater than the cut-off value, the cryptographic can be continually overused by a sensor exceeding the time limit t without wasting energy and exerting efforts in exchanging new keys. The probability and threshold values are dependent on the power and size of the keys of a cryptographic algorithm, thus confirming the flexibility (due to its fitness in variable situations and nature of the algorithm) and easy applicability. It can be used by a network administrator to assess the performance of multiple algorithms and choose the one that meets the network's basic security standards while also consuming the fewest resources of the network. This paper addresses the following research questions:

How to select an appropriate algorithm for WSN?

What metrics should be utilized to evaluate cryptographic algorithms' performances?

What criteria are required for metrics calculation?

What are the hypotheses?

In this research, an analytical model has been created to assess the cryptographic algorithms' KSP, which was engaged in comparing numerous cryptographic algorithms for which the desired level of KSP was chosen by the network administrator and was utilized as a cut-off or threshold. Later, the KSP of multiple algorithms was compared by this analytical framework which enabled the network administrator to choose the optimal algorithm exceeding the threshold level of KSP and using the least resources of the network.

IV. ENCRYPTIONS ALGORITHMS PERFORMANCE ANALYSIS MODEL

The sensor network's sensor accumulates the data, which is transferred to either of its adjacent sensors on the basis of the routing mechanism of the network. This is a repetitive process to be done until the data is received at the base destination. Encryption technology is used to maintain the security of the data which is delivered over the network. The ceaseless functionality of this encryption mechanism requires the exchange of safety parameters (private and public keys and their sizes) between all the nodes of the WSN on a regular basis. These control message distributions via a security gateway add to the load on a resource node with a small size limit. This study targets to find an effective security mechanism for WSN while minimizing control message broadcasting.

In this study, Key Strength Probability (KSP) has been used as the fundamental measure to compare multiple safety algorithms. KSP can be defined as the possibility of an algorithm's cryptographic key to remaining unveiled and safe from a fierce, forceful attack for time (t) [15]. KSP is the counterpart of the probability of success from an attack after (t) time. Hence,

$$KSP = 1 - P_{SA}(t) \qquad (1)$$

Where $P_{SA}(t)$ is the success prospect of an attack after the time (t), and thus, $P_{SA}(t)$ can be found as [15]:

$$P_{SA}(t) = \frac{k(t)}{2^s} \qquad (2)$$

Where $k(t)$ implies the number of keys inaccessible to an adversary for being tried until the time (t), and (s) is the strength of the key in bits. $k(t)$ can be explored by multiplication of the number of keys tried by an adversary per unit of time (f), by time (t), then

$$k(t) = f.t \qquad (3)$$

(1), (2), and (3) reveal the following derivation [15]:

$$KSP = \begin{cases} 1 - \frac{f.t}{2^s}, & 0 \le t \le \frac{2^s}{f} \\ 0, & else \end{cases} \qquad (4)$$

Where the t implies, the time lapsed since the activation of the key by a said sensor node. Due to the activation of the keys of each node at separate moments, they have individual values of t. The parameter s which is dependent on the algorithm can be found in the literature for any symmetrical or asymmetrical algorithm and, if it is unknown for a particular algorithm, s harmonizes with the size of the key (in bits) [15]. Lastly, the parameter f can be identified on the basis of the algorithm that resembles the higher key test throughput, which is available publicly. Note that $0 \le KSP \le 1$, so a threshold can be set for KSP (th_{ksp}) where the data is regarded as agreeable and may be transferred from the present sensor to another one in the vicinity if $KSP \ge th_{ksp}$, where $0 \le th_{ksp} \le 1$, and is described on the basis of the data sensitivity and the desired security level. Data acceptance probability (P_{DA}) at a sensor can be defined on the basis of the above discussion as the possibility that the data of a particular sensor is accepted and broadcasted to an adjacent sensor or the base station as KSP of that sensor is greater than or equal to th_{ksp}

$$P_{DA} = P_r(KSP \ge th_{ksp})$$

Where $P_r(x \ge y)$ represents the possibility that $(x \ge y)$, and using (4), P_{DA} can be derived as follows:

$$P_r(KSP < th_{ksp}) = P_r\left(1 - \frac{f.t}{2^s} < th_{ksp}\right) \qquad (5)$$

$$= P_r\left(t > (1 - th_{ksp})\frac{2^s}{f}\right) \qquad (6)$$

$$= 1 - P_r\left(t \le (1 - th_{ksp})\frac{2^s}{f}\right) \qquad (7)$$

and since $P_r(KSP \ge th_{ksp})$ is the counterpart of $P_r(KSP < th_{ksp})$, then

$$P_{DA} = P_r(KSP \ge th_{ksp} = 1 - P_r(KSP < th_{ksp} \qquad (8)$$

From (8) and (7), we get:

$$P_{DA} = P_r\left(t \le (1 - th_{ksp})\frac{2^s}{f}\right) \qquad (9)$$

The t implies the time-span since the activation of the key in the said sensor node; however, it can be assumed on the basis of WSN's nature that the network has identical sensors and each sensor's time t is variable than the other sensors. Development of an analytical model for assessing P_{DA} and simplifying the analysis, t can be estimated with the help of a random attribute/variable aligning with right-hand side distribution; for example, gamma distribution or positive uniform distribution. Later, this estimation can assist in numerical evaluation of P_{DA} in (9). For using the newly devised model for comparing variable encryption algorithms, a threshold ($th_{P_{DA}}$) can be set for P_{DA}, wherein algorithms with $P_{DA} \ge th_{P_{DA}}$ can be optimally utilized in the network, and the algorithm that uses the least amount of resources of the network can be chosen out of these algorithms.

Implication

The analytical framework created in the former section has been engaged in this section, and the below-mentioned assumptions have been used for simplification of its implementation:

(1) All sensor nodes are alike

t is independent of remaining sensors in each sensor

t is an arbitrary variable that follows the distribution of gamma with parameters α and β wherein α is the shape criterion and β is the rate criterion of (t) and (1/ β) is the scale criterion.

P_{DA} may be examined with the use of (9) as gamma's Cumulative Distribution Function (CDF).

$$P_{DA} = \frac{1}{\Gamma(\alpha)} \gamma(\alpha, \beta.((1 - th_{ksp}).\frac{2^s}{f})) \quad (10)$$

Where α is the shape specification and $(\alpha > 0)$, β is the rate specification and $(\beta > 0)$, $\Gamma(\alpha)$ is the function of gamma that can be derived as:

$$\Gamma(\alpha) = \int_0^\infty X^{(\alpha-1)}.\ e^{(-x)}\ dx \quad (11)$$

And $\gamma(x, y)$ is the lower incomplete gamma that can be extracted as:

$$\gamma(x, y) = \int_0^y W^{(x-1)}.\ e^{(-w)}\ dw \quad (12)$$

The parameters like α and β can be chosen for accurate approximation of (t), which needs to be discussed in detail in future studies, whereas the criteria like s, f, and th_{ksp} can be discussed earlier. With the use of the model developed in the former section and the assumptions derived thereafter, we get

$$P_{DA} = \frac{\int_0^{\beta(1-th_{ksp})\frac{2^s}{f}} W^{\alpha-1} e^{\alpha}\ dw}{\int_0^\infty W^{(\alpha-1)}.\ e^{(-w)}\ dw} \quad (13)$$

However, a comparison between variable cryptography algorithms can be made with the help of (13).

V. RESULTS AND DISCUSSION

With the aid of the model built in the prior section, multiple algorithms of encryption used for balanced security of WSN having the strength (s=56, s=57, and s=57) have been analyzed herein. The adaptability of gamma distribution has been depicted in **Fig. 1**, which assists in the approximation of time *t*. As portrayed in the figure, the distribution of time *t* is largely affected by the rate and the shape. This adaptability assists in approximating *t* with utmost precision.

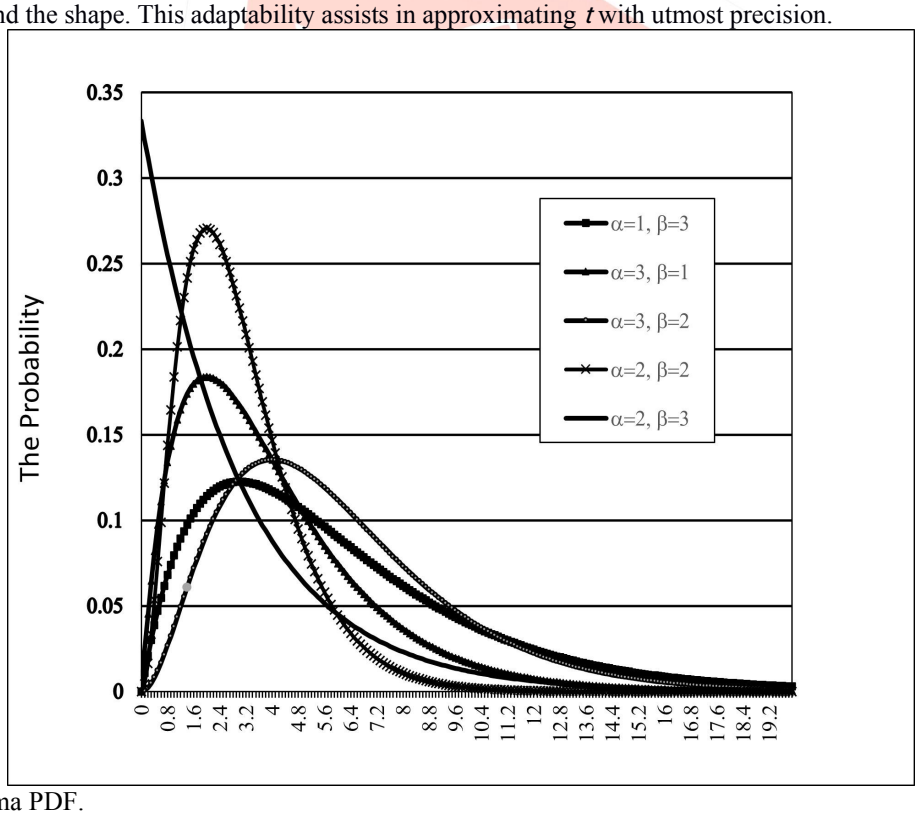

Figure 1. Gamma PDF.

The probability of accepting data vs. KSP threshold is depicted in **Fig. 2**, which shows that an increase in the threshold causes a decrease in the probability of data acceptance. Additionally, the increase in the probability of data acceptance also grows with the increase in the level of strength, as shown in the figure. As shown in the illustration below, we can specify the algorithms that meet the appropriate criteria of security by setting a threshold each for data acceptance probability as well as KSP probability. For instance, if $th_{P_{DA}} = 0.75$ and the desired th_{ksp} =0.79, then the algorithm having (s=57) or the algorithm with (s=58) can be used instead of the algorithm with strength (s=56) depending on the algorithm that requires the least amount of resources as explored in the literature.

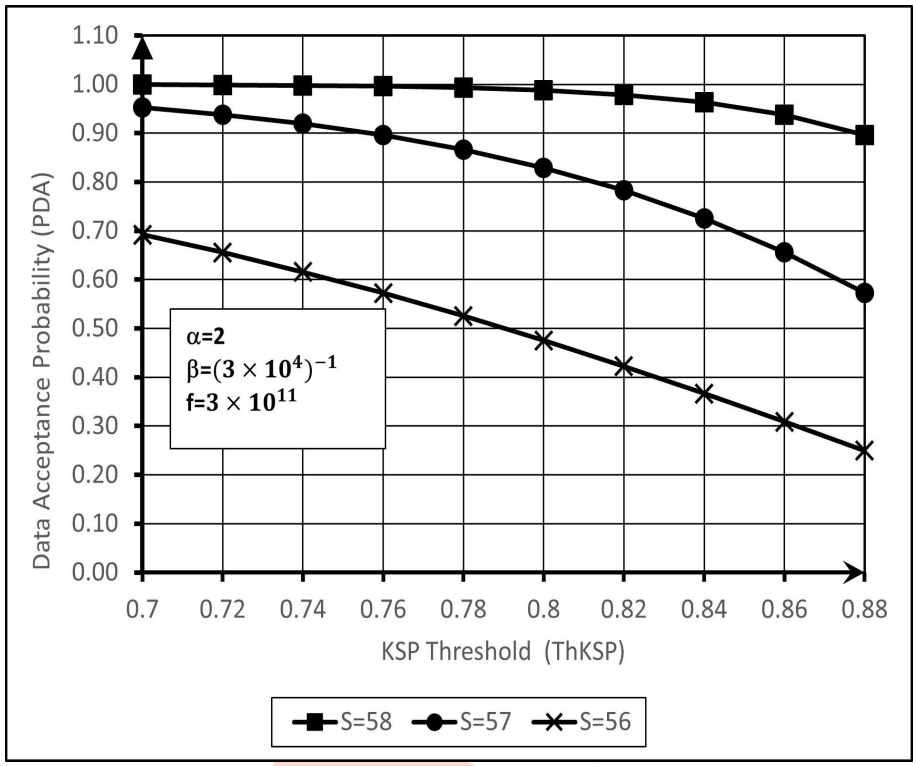

Figure 2. Data Acceptance Probability (PDA) vs KSP Threshold.

The impact of alterations in the parameters of scale and shape of the new model have been depicted in **Fig 3 and 4**, wherein the distribution of (t) along with the mean and the variance of (t) are directly impacted by these attributes.

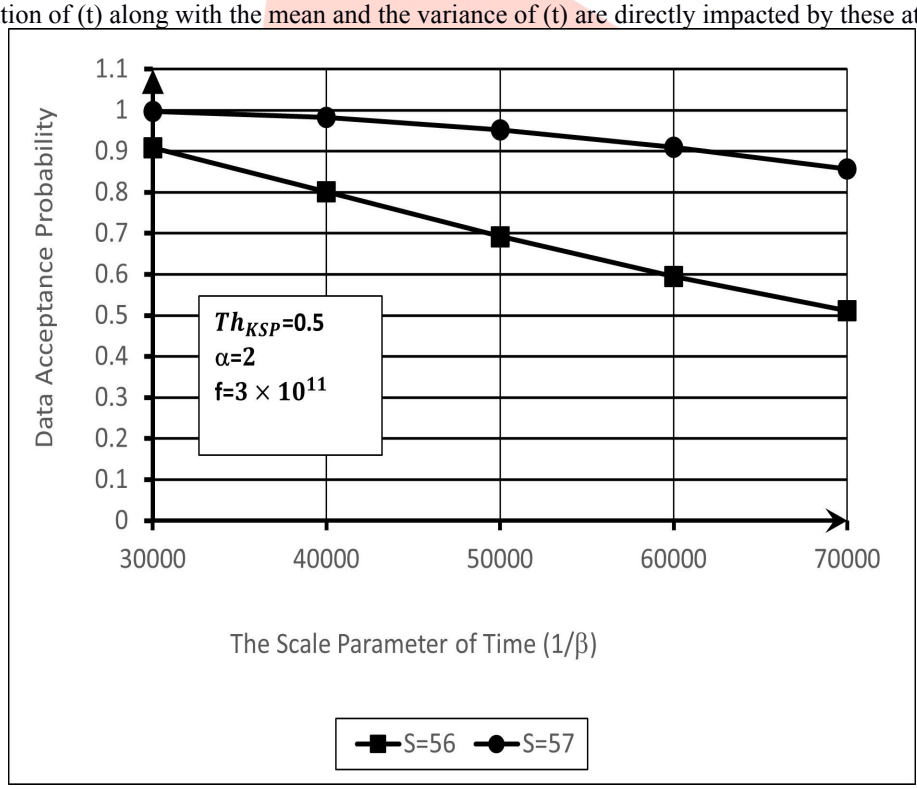

Figure 3. Data Acceptance Probability vs The Scale Parameter of Time (1/β).

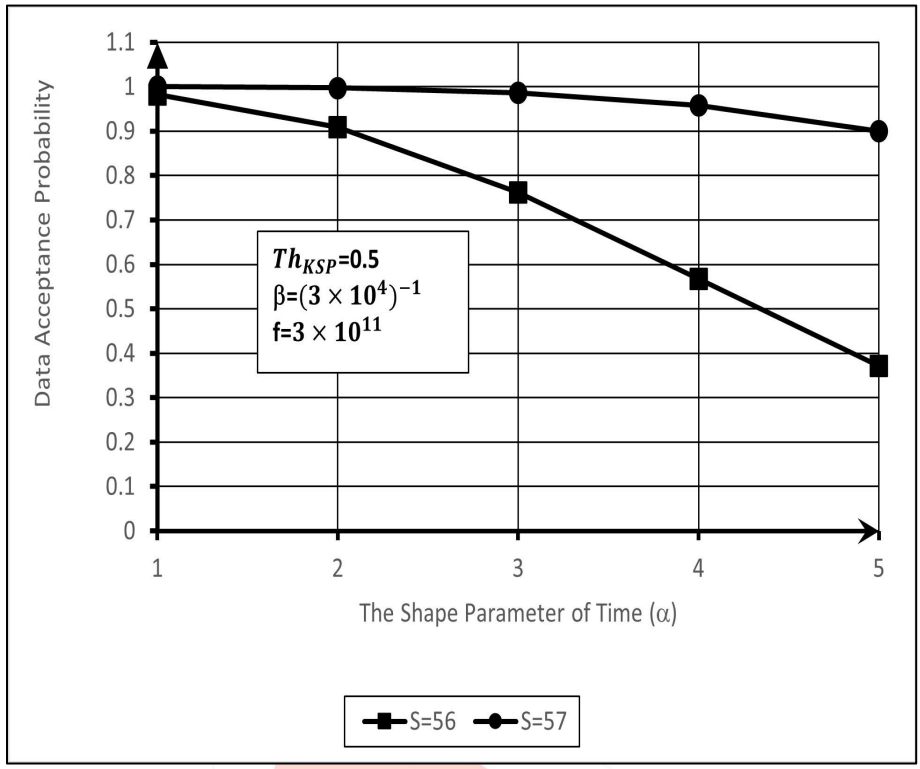

Figure 4. Data Acceptance Probability vs The Shape Parameter of Time (α).

VI. CONCLUSIONS

WSN supports a variety of encryption techniques. However, because of the restricted availability of resources available in this network, it becomes tedious to choose the algorithm for this study. The primary contribution of this study is an analytical framework that has been devised to assess and compare the performance of numerous cryptographic algorithms rather than struggling with complex simulation approaches. The magnitude of the key strength probability of KSP is known to vary on the basis of factors such as the algorithm's security strength, the size of the key, and the category of a cryptography algorithm. It is determined that just because an algorithm has the greatest level of strength does not make it the best option; rather, a simpler algorithm with lower strength that conserves resources of the network may be utilized to match the needed degree of security. An additional contribution of this study is the introduction and usage of data acceptance probability as a new parameter for comparing algorithms analytically.

FUNDING

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENT

The authors are grateful and acknowledge the assistance of the SNCS Research Centre based at the University of Tabuk, Saudi Arabia.

REFERENCES

[1] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," Sensors., 2009, vol. 9, pp. 6869–6896. https://doi.org/10.3390/s90906869.

[2] S. Nithyanandh, and V. Jaiganesh, "Wireless sensor networks overview and study of various applications and environmental factors in WSNs," IOSR J. Comput. Eng., 2020, vol. 6, pp. 24–27.

[3] V. Potdar, A. Sharif, and E. Chang, "Wireless Sensor Networks: A Survey. in 2009 International Conference on Advanced Information Networking and Applications Workshops," 2009, pp. 634–641.

[4] A. Stetsko, L. Folkman, and V. Matyáš, "Neighbor-based intrusion detection for wireless sensor networks," In Proceedings of the 2010 6th International Conference on Wireless and Mobile Communications, 2010, pp. 420–425.

[5] G. Sharma, S. Bala, and A. K. Verma, "Security frameworks for wireless sensor networks-review," Proc. Technol., 2012, vol. 6, pp. 978–987. https://doi.org/10.1016/j.protcy.2012.10.119.

[6] M. Panda, "Performance analysis of encryption algorithms for security," In Proceedings of the 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 278–284.

[7] S. Tom, and J. Simon, Public Key Algorithms. Cryptography for Developers, Nethrland, Elsevier, 2007, pp. 379–407.

[8] J. Thakkar, "Types of Encryption: What to Know About Symmetric vs Asymmetric Encryption," Available online: https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/.

[9] X. Zhou, and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," In Proceedings of the Proceedings of 2011 6th international forum on strategic technology, 2011, pp. 1118–1121.

[10] M. A. Simplício Jr, P.S. Barreto, C. B. Margi, T. C. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," Comput. Netw., 2010, vol. 54, pp. 2591–2612. https://doi.org/10.1016/j.comnet.2010.04.010.
[11] M. Dener, "Comparison of encryption algorithms in wireless sensor networks," In Proceedings of the ITM Web of Conferences, 2018, pp. 1–5.
[12] W. Elgenaidi, T. Newe, E. O'Connell, D. Toal, G. Dooly, and J. Coleman, "Memory storage administration of security encryption keys for line topology in maritime wireless sensor networks," In Proceedings of the 2016 10th International Conference on Sensing Technology (ICST), 2016, pp. 1–4.
[13] V. A. Memos, K. E. Psannis, Y. Ishibashi, B. G. Kim, and B. B. Gupta, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework," Future. Gener. Comput. Syst., 2018, vol 83, pp. 619–628. https://doi.org/10.1016/j.future.2017.04.039.
[14] K. Ravi, R. Khanai, and K. Praveen, "Survey on pairing based cryptography for wireless sensor networks," In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1–4.
[15] A. Ramos, "Sensor data security level estimation scheme for wireless sensor networks," Sensors. 2015, vol. 15, pp. 2104–2136. https://doi.org/10.3390/s150102104.