ISSN: 0067-2904

Improving Security in Wireless Sensor Networks: A New Key Pre-Distribution Approach with Taylor Series

Basim Najim Al-din Abed[1], Sura Abed Sarab[2*]
[1]Dpartment of Computer science, College of Science, University of Diyala, Diyala, Iraq
[2]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Received: 30/6/2024 Accepted: 24/9/2024 Published: 30/10/2025

Abstract

Ensuring robust authentication is essential in Wireless Sensor Networks (WSNs) to protect sensitive data transfer between nodes. This paper proposes the use of mathematical implementations to enhance the security and complexity of secret data transmission between nodes, thereby providing a robust communication system. Additionally, it proposes a new mathematical implementation as an authentication model based on the Taylor expansion sequence. This strategy allows secure communication between any two nodes to prevent the malicious node from stealing the data or hacking the secret information from any node on the network. The proposed solution is based on unique parameters carried by any two communicating nodes in the network. These nodes exchange specific parameters, subsequently using the partial sum of a geometric sequence to generate an authentication code. This technique offers secure communication between nodes over the internet, which improves overall network security.

Keywords: wireless sensor networks, Taylor expansion, Cryptography, Authentication, one-way function.

تحسين الأمان في شبكات الاستشعار اللاسلكية: نهج رئيسي جديد لما قبل التوزيع مع سلسلة Taylor

باسم نجم الدين عبد[1] , سرى عبد سراب*[2]
قسم علوم الحاسوب, كلية العلوم , جامعة ديالى, ديالى , عراق
قسم علوم الحاسوب, كلية العلوم , جامعة بغداد, بغداد , عراق

الخلاصه

يعد ضمان المصادقة القوية أمرا ضروريا في شبكات الاستشعار اللاسلكية (WSNs) لحماية نقل البيانات الحساسة بين العقد. لتوفير نظام اتصال قوي ، تقترح هذه الورقة استعمال التطبيقات الرياضية لزيادة الأمان والتعقيد للبيانات السرية التي يتم نقلها بين العقد. بالإضافة الى اقتراح تطبيقا رياضيا جديدا كنموذج اثبات أصاله جديد ، بناء على تسلسل توسع تايلور. تسمح هذه الإستراتيجية بالاتصال الآمن بين أي عقدتين ، لمنع العقدة الضارة من سرقة البيانات أو اختراق المعلومات السرية من أي عقدة على الشبكة. يعتمد الحل المقترح على المتغيرات الفريدة التي تحملها أي عقدتين متصلتين في الشبكة. تتبادل هذه العقد متغيرات محددة ، والتي

*Email: suraaljanaby8484@gmail.com

تستعمل لاحقا لإنشاء رمز اثبات الاصالة باستعمال المجموع الجزئي لتسلسل هندسي. توفر هذه التقنية اتصالا آمنا بين العقد عبر الإنترنت ، مما يحسن أمان الشبكة بشكل عام.

1. Introduction

Wireless sensor networks (WSNs) are made up of thousands of nodes, each containing a sensor. Sensor nodes are small, require location memory, are cost-effective with limited power sources, and limit control. WSNs are rapidly gaining popularity due to their simple solutions for a variety of real-world problems [1]. The essential idea of a sensor system is to disperse a small number of detection devices suitable for certain changes in events/boundaries and to talk with other devices for many purposes, such as research, biology assessment, and goal pursuit [2]. The lack of information storage and force sensor systems creates significant asset demands. There are deterrents to the use of conventional PC secrecy procedures in the WSN. Security safeguards are more enthusiastically implemented in WSNs due to the temperamental correspondence channel and unattended activity [3]. Accordingly, these systems require a few one-of-a-kind security policies. Cryptography, steganography, and different nuts and bolts of system security, with their appropriateness, can be utilized to address the issues of basic security in WSN [4].

Numerous specialists start addressing the amplifying of the preparing abilities, vitality sparing of sensor nodes, and making sure against the attackers [5]. Security of the system includes the qualities of confirmation integrity, privacy, anti-playback, and nonrepudiation. More danger of the secure transmission of the data over the system, which has expanded more reliance on the data given by the increasing of the systems [6]. Several steganography, cryptography, and different methods are utilized that are known for the protected transmission of various kinds of data over systems. Cryptography procedures conceived for conventional wired systems are not plausible to apply straightforwardly for the remote sensor systems [7].

The WSNs are made up of several sensors that seriously suffer from a shortage of processing, memory, and battery life. Any encryption scheme used on WSNs must transmit more bits, requiring more memory, processing power, and battery life—all important resources for extending the sensor's lifespan [8]. By utilizing the security components, for instance, the encryption may also be broadened to address the jitter, delay, and bundling issues in remote sensor systems [9]. Implementing cryptography schemes on WSNs raises important questions, including how to produce or vanish keys [10].

One specific issue is how to change the keys from an opportunity to a time when the encryption is insignificant or there is no connection to the sensors. There are many numerous issues, such as how the keys can be repudiated, doled out to other sensors added to organize, or restored to ensure the system has good security. Many researchers have made considerable efforts to meet these challenges by designing secure and dependable authentication mechanisms [11].

2. Related Works

Alwan et al. [12] propose a new approach involving the generation of random pool keys. According to the original parameters and conditions, which are subsequently used to store individual segments through using Taylor series as a random key generation technique. Performance evaluation of this approach includes tests, for example, mean square error, peak signal-to-noise ratio, and structural similarity index measure to evaluate its effectiveness. The National Institute of Standards and Technology determined the validity of the random key. Ongoing research is investigating the time required for decryption and encryption processes.

The security of the encryption methodology is attributed to the unpredictability of the chaotic attractor. Moreover, the encryption approach uses metrics like correlation coefficient, Shannon entropy, and histogram to evaluate its success. This paper finds that the new encryption approach consistently performs well by adding mechanisms to enhance protection against known or selected explicitly coded attacks. Results also indicate both decoding and encoding of this encryption schema are time-efficient.

Chan et al. [13] present three novel key transfer strategies that use a systematic prior distribution of the random keys going to every node. First, the q-composite key method changes the chance of a wide-domain network attack, which makes random key pre-distribution more effective against few-domain attacks. Secondly, the multi-path reinforcement method demonstrates how to strengthen protection between two nodes by leveraging the protection of other links. Finally, it can submit a randomly generated key structure that preserves the privacy of the reminder network during node removal, enables quorum-based elimination, and enhances the Koblitz encryption method with node-to-node authentication.

Abirami et al. [14] propose elliptic curve cryptography (ECC) to enhance the protection scheme. A comparative analysis between the proposed model and existing models revealed the proposed model's superior efficiency in terms of security enhancement. The proposed model guarantees confidentiality through encryption techniques, ensures integrity via hashing methods, and establishes authenticity and non-repudiation by incorporating digital signatures [14].

Abirami et al. [15] propose a new method that merges reactive and reactive systems. The active side uses machine learning-dependent classification algorithms that predict attacks, while this active component is used in the attack prediction to identify the attacker. Authenticity and confidentiality are ensured through an encryption scheme by encrypting reports from the active module prior to decryption in the reactive module. In this study, the proposed ECC that depends on a security model is compared with various present safety systems. Furthermore, machine learning-based multiple classification algorithms are compared to determine the optimal strategy for the proposed network design. Performance metrics such as accuracy, recall, precision, and F1 value are utilized to evaluate these algorithms, with the analysis recommending the adoption of the Extreme Gradient Boosting (XGB) technique for the Network Forensic Framework implementation.

Hoobi et al. [16] developed a comprehensive multilevel cryptography model and evaluated it using three distinct cases. These cases involve the use of the RC5 algorithm alone in Case 1, an examination of the combined use of RC5 and two-fish algorithms in Case 2, and a series of three active algorithms (RC5, fish two, and Modified Snake) in Case (3). Analysis of the results indicates that case (3), which applies three effective algorithms sequentially for data encryption, is the preferred approach. This chapter provides demonstration examples of different mixtures of symmetric key cryptography algorithms, such as RC5, two fish, and Modified Serpent. A comparative test of the three cases is performed using tools such as brute force attacks, entropy, autocorrelation, and other methods.

Eschenauer et al. [1] allocated sensor nodes an arbitrary subset from a major key in the system's key pool sending. The primary key advances pre-alpha-ever. Organization after two contiguous, nevertheless, can manufacture sensor nodes between them the key if they had at any rate one basic component in their key rings. Regrettably, these key pools are highly susceptible to such arrangements.

Afianti et al. [17] proposed a multi-user dynamic cipher puzzle planted with Tiny Set, where the recent system supply ensured privacy and lightweight DoS resistance in multiuser WSN authentication. The proposed scheme and RC5 encryption method, when combined with

the elliptic curve digital signature method, resulted in a 36% increase in security when compared to a Count Bloom filter.

Ghani et al. [18] proposed an enhanced symmetric key-based authentication protocol for IoT-based WSN. The proposed protocol has counter-user tracing capabilities, stolen verifiers, and DoS attacks. The proposed protocol has an efficiency of 52.63% compared to the original protocol.

Manasrah et al. [19] proposed the BLU decomposition method, which ensures that any two linked nodes must participate in a shared key before initiating communication. The suggested method outperforms the existing approaches.
To provide a clearer and more organized presentation of the research landscape, Table 1 below summarizes the key details of these studies:

Table I: SUMMARY OF KEY STUDIES ON ULTRA-LIGHTWIGHT S-BOX GENERATION VIA QUANTUM INSPIRATION

Study	Method	Key Contributions	Limitations
Alwan, et al. (2023)	Using Taylor series as a random key generation technique.	Enhanced security properties	High computational requirements
Chan, et al. (2003)	Koblitz encoding with ECC cryptography for Random key pre-distribution	Save the privacy of sensor networks	Challenges in maintaining consistent security
Abirami, et al. (2024)	Proposed EEC encryption techniques	Enhance the Security of network	Lack of practical implementation framework
Abirami, et al. (2023)	Machine learning that predicted attack.	Security Authenticity and confidentiality are ensured	High computational complexity
Hoobi, et al. (2024)	Different mixture of symmetric key cryptography algorithms	Develop a multilevel cryptography model	Limited focus on specific Symmetric key algorithm design improvements
Eschenauer, et al. (2003)	Allocated sensor nodes arbitrary subset from a major key	Enhanced security properties	Lack of empirical analysis on efficiency and scalability
Afianti, et al. (2019)	Multi-user dynamic cipher puzzle planted with Tiny Set	Ensured privacy and lightweight DoS resistance in multiuser WSN authentication	Challenges in maintaining consistent security
Ghani, et al. (2019)	Symmetric key-based authentication protocol for IoT-based WSN	Enhanced Security so the Efficiency of 52.63% compared to the original protocol	High computational complexity
Manasrah, et al. (2019)	BLU de-composition method, so any two linked nodes participate a popular key between nods	Strong security properties	Lack of practical implementation framework

3. Authentication

In WSNs, authentication plays a vital role in guaranteeing the confidentiality and accuracy of data. Since WSNs are frequently installed in sensitive locations, any tampering or illegal access might have serious repercussions [20]. Prior to being utilized for higher-level applications, every package entering the remote sensor organization needs to be verified. We

can use one bounce unicast, multi-jump unicast, and communication for verification. Authentication involves verifying the identity of a user or device to confirm their authenticity. It is an important part of network security in many contexts [21].

3.1 Verification with correspondence design

There is sort of correspondence in WSNs dependent on which confirmation schemes are developed [1]:

1) One-bounce confirmation: A common connection layer key is required between neighboring nodes. The main actualized design, which provides confirmation and encryption, is a small section. Even though it is full implantation, it doesn't talk about how to set up connect layer keys.

2) Multi-jump Authentication: Start to finish shared keys support multi-bounce confirmation. In any case, it falls flat on the off chance that one of the nodes in the way is undermined.

3) Broadcast Authentication: On the off chance that source code requires some message, like order, it communicates the message. For this situation, every parcel that is communicated ought to be verified with the goal that no bogus information is embedded. We employed this approach in our work.

3.2 Steps Required for Authentication

Before applying the verification procedure, there are a few essentials that need to be finished. The security in a remote sensor organization is exceptionally reliant upon the cryptographic keys. The administration of these keys is a troublesome undertaking. The key administration is creating, putting away, moving, and utilizing the cryptographic keys. Few stages are there to apply [22]:

1) Deployment of systems and keys networks are conveyed in focused zones, and the number of keys required should be determined.

2) Establishment of keys is set up between nodes that are happy to have the correspondence.

3) Authentication Protocol On the off chance that any node needs to join the system, it needs to pass a few conditions offered by the verification convention. Furthermore, it is contingent upon the node's request for inclusion.

4) Node expansion/erasure: the nodes ought to be added to the system on the off chance that they are carrying on for the applied validation convention. It is the duty of the validation convention to permit node to begin protected correspondence with other part nodes. The failing or pointless nodes ought to likewise be erased by this procedure.

3.3 Audit attack in WSNs

The small spread nodes are vulnerable to various types of attacks. There are two classes of assaults. Attacks against fundamental activity: Attacks against security components occur at various stages and utilize diverse methodologies [23].

3.3.1 Node Capture:

The keys and other made-about data can be taken by straightforwardly catching the node with the assistance of physical assaults. Node-catch assaults are a combination of uninvolved, dynamic, and physical attacks, typically carried out by an intelligent attacker. For instatement or arrangement an assault, the enemy can accumulate data about the WSN by listening in on message exchanges during correspondence, nearby to a utilizing outer gadget. Regardless of whether message information is encoded, the enemy can separate secure data about the system activity, successfully finding out about the system structure and capacity.

3.3.2 Bogus Node:

The phony information can be embedded by the untouchable by utilizing bogus nodes. This node replicates the existing node and attempts to pass itself off as the genuine one.

3.3.3 Malfunctioning of node:

A node failure can be risky because it infuses bogus data into the system. The entire system may be useless.

3.4 Sybil Attack:

Area-based directing convention is experienced Sybil assault. The Sybil assault creates multiple characters on a single node. The node needs to trade the data with neighbors but can't trade because of various characters of neighbor. If authentication is utilized, at that point this assault can be forestalled.

3.5 Sinkhole Attack:

The traffic of the system is helped through the undermined node called the sink. The undermined node is made appealing and goes about as an amazing node. Along these lines, different nodes effectively pass information to this sink node and result in organized disappointment.

4. Methodology

The Taylor series or Taylor expansion of a function can be represented as an infinite sum of terms in the Taylor series, where each term involves the derivatives of the function at a single point. The Taylor series gives the function (f(m)) around the point (a) in a normal form [24-27]:

$$f(m) = f(b) + f^{(1)}(b)(m-b) + \frac{f^{(2)}(b)}{2!}(m-b)^2 + \frac{f^{(3)}(b)}{3!}(m-b)^3 + \cdots + \frac{f^{(d)}(b)}{d!}(m-b)^d \quad \ldots\ldots\ldots (1)$$

The methodology used in the proposed method consists of the following steps:

1. **Wireless Sensor Network Layout:**

- Sensor Nodes: Small circles distributed across the field indicate sensor nodes. These are the wireless sensor network's individual sensors, each of which is responsible for monitoring and collecting data.
- The larger circle indicates the base station. It serves as the network's central hub, coordinating communications and distributing keys to sensor nodes.
- Dashed lines connect sensor nodes to the base station and each other, symbolizing communication links for data and key exchange.

2. **Polynomial Generation:**

Label the block as "Polynomial Generation." This block has a polynomial function:

$$F(x, y) = a_0 + a_1 x + a_2 x^2 + \cdots \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

This polynomial serves as the basis for creating keys for each sensor node. The base station determines the coefficients a_0, a_1, a_2, and so on, which are kept secret.

3. **Taylor Series Expansion:**

- **Block Label:** "Taylor Series Expansion."

- **Content**: This block displays the Taylor series formula:

$$F(x+h) = f(x)+(f'(x))/1!\ h+(f''(x))/2!\ h^2+\cdots. \quad \ldots\ldots\ldots\ldots\ldots \quad (3)$$

At various places, which is critical for delivering unique key fragments to nodes.

- **Arrow**: There is an arrow from the Polynomial Generation block to this block, suggesting that the polynomial formed in the first step is expanded with the Taylor series.

4. Distribution of keys to nodes:

- **Arrows to sensor nodes.** Several arrows in the Taylor Series Expansion block point to different sensor nodes. Each arrow depicts the distribution of a unique key fragment to each sensor node.
- **Label**: The key fragments are denoted by

$$K_i = f(x_i, y_i) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

where x_i and y_i are unique values assigned to each node. These fragments are from the enlarged Taylor series and are unique to each sensor node.

5. **Shared Key Calculation:**

- **Block Label:** "Shared Key Calculation."
- **Content*:*** This block is located between two sensor nodes and displays the formula:

$$K_{shared} = f(x_i,y_i)+f(x_i,y_i). \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (5)$$

This depicts the mechanism by which two sensor nodes combine their key fragments to create a shared key for safe communication.

- **Arrows:** The two sensor nodes' signs point to this block, indicating that both nodes contribute to the creation of the shared key.

6 Secure Communication:

- **Dashed lines between sensor nodes** indicate secure communication connections. These channels encrypt and safeguard the data sent between the nodes using the previously determined shared keys.

7. Base Station Role:

- **Base station:** The base station distributes the polynomial and key fragments to each sensor node, as seen in the diagram. To ensure security over time, it may also be helpful to refresh or update these keys as needed.

The base station creates a polynomial and uses a Taylor series to deliver unique key fragments to each sensor node. Sensor nodes use key fragments to generate shared keys with neighbors. These shared keys allow for safe communication between sensor nodes in the wireless sensor network. This procedure assures that even if a few nodes are hacked, the overall security of the network is maintained due to the uniqueness and mathematical features of the keys obtained from the Taylor series. To calculate the energy, power, and time consumption of this technology and then present the findings in tables and curves to demonstrate its originality, we'd need to consider numerous aspects unique to your wireless sensor network (WSN). Here is a general method.

Implementation:

1. Modeling Energy Consumption

Energy consumption in a WSN typically includes:

Communication Energy (Ecomm): Energy used for transmitting and receiving data (Energy for Communication). The energy consumed in communication can be modeled as:

$$E_{comm}=E_{tx}+E_{rx} \quad \text{......} \quad (6)$$

Where: E_{tx} is the energy required to transmit data, E_{rx} is the energy required to receive data.

Typically:

$$Etx = l \times (E_{elec}+E_{amp} \times d\ n) \quad \text{......} \quad (7)$$

$$E_{rx}=l \times E_{elec} \quad \text{......} \quad (8)$$

Where: l is the length of the data packet, E_{elec} is the energy per bit for transmission/reception, E_{amp} is the energy for amplification, d is the distance between nodes, n is the path-loss exponent (typically 2 for free space, 4 for multipath).

Computation Energy (E_{comp}): Energy consumed during key generation, expansion (using Taylor Series), and key distribution. For the Taylor Series expansion and key generation:

$$E_{comp}=N \times E_{operation} \quad \text{......} \quad (9)$$

Where: N is the number of operations (addition, multiplication, etc.), $E_{operation}$ is the energy cost per operation.

2. Modeling Power Consumption

Power consumption P is given by:

$$P = \frac{E}{T} \quad \text{......} \quad (10)$$

Where E is the energy consumed, And T is the time taken for the process (computation or communication).

3. Modeling Time Consumption

Time consumption depends on:

Transmission Time (T_{comm}): $T_{comm} = \frac{l}{B}$ ...... (11)

Where B is the bandwidth of the channel.

Computation Time (T_{comp}): Based on the processing speed of the node's CPU and the complexity of operations.

Example: Let's assume some example parameters:

Transmission Parameters:

- $l=512$ bits
- $E_{elec}=50$ nJ/bit
- $E_{amp}=100$ pJ/bit/m²
- $d=10$ meters
- $n=2$

Computation Parameters:

- *N=1000 operations*
- *Eoperation=10 pJ/operation*
- *CPU speed: 1 MHz*

Using these, we can compute energy, power, and time consumption for different scenarios as shown in Table 2.

Table 2: Energy, Power, and Time consumption for different scenarios

	Energy Consumption	Power Consumption	Time Consumption
Component	**Value per Node (nJ)**	**Value per Node (nW)**	**Value per Node (ms)**
Transmission (E_{tx})	3.072×10^{-5}Joules	0.06 Watts	0.000512 seconds
Reception (E_{rx})	2.56×10^{-5} Joules	0.05 Watts	0.000512 seconds
Computation (E_{comp})	1×10^{-8} Joules	1×10^{-5} Watts	0.001 seconds
Total (E_total)	**5.633×10^{-5} Joules**	**0.11001 Watts**	**0.002024 seconds**

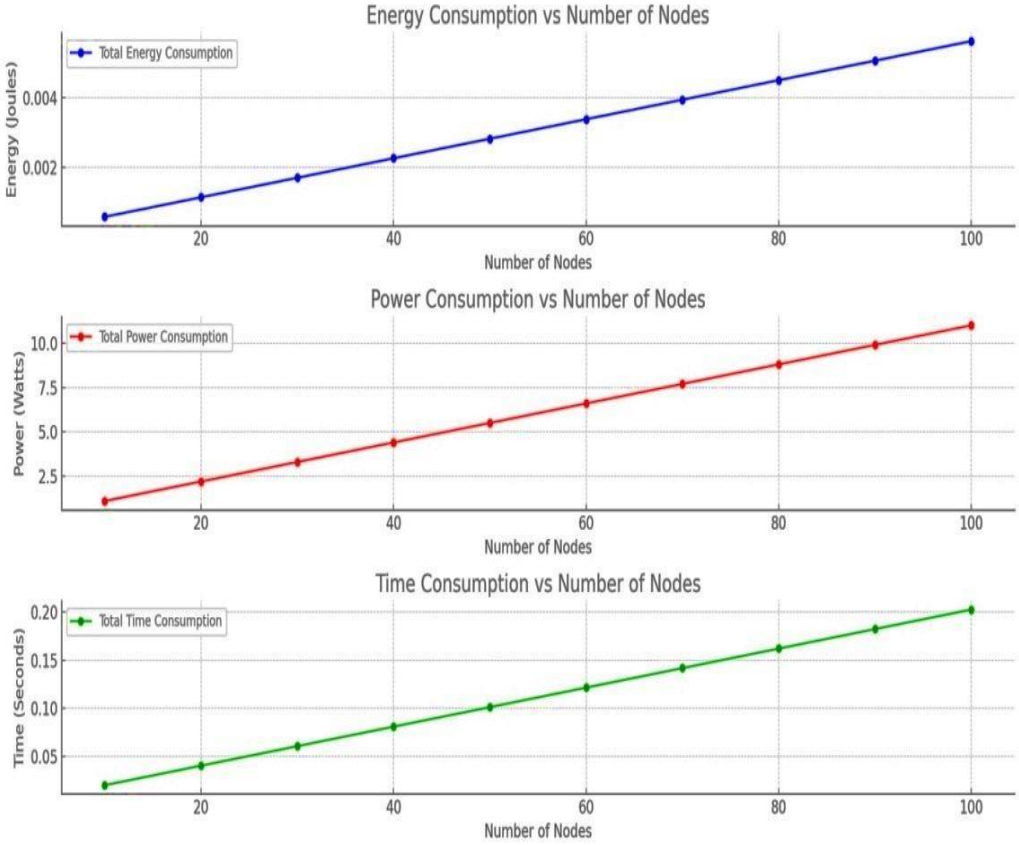

Figure 1: Proposed schema

In the figure above, we can see the total energy consumption as a function of the number of nodes in the network. The number of nodes influences the total power consumption. The number of nodes determines the total time consumption. The curves in the generated plot illustrate the relationship between the number of nodes in the network and the overall energy, power, and time consumption.

This analysis and visualization underscore the scalability and efficiency of the key pre-distribution method using Taylor series in a wireless sensor network. The linear trends indicate that the method scales predictably with network size, making it suitable for large-scale deployments.

To plot the curve for the probability of two nodes sharing at least one key when each node randomly chooses τ spaces from a total of ω spaces, we can use the following approach:

Probability Calculation

The probability that two nodes **do not** share any keys is:

$$P_{no\ share} = (\frac{\omega-\tau}{\omega})^{\tau} \quad \text{.....(12)}$$

Thus, the probability that they share **at least one** key is:

$$P_{share}=1-P_{no\ share} \quad \text{..... (13)}$$

$$P_{share} = 1 - (\frac{\omega-\tau}{\omega})^{\tau} \quad \text{..... (14)}$$

Let's assume some values for τ and ω and plot the curve. We'll vary τ while keeping ω constant and plot the probability P_{share} .

Figure 2, plot the curve for different values of ω to see how the probability changes.

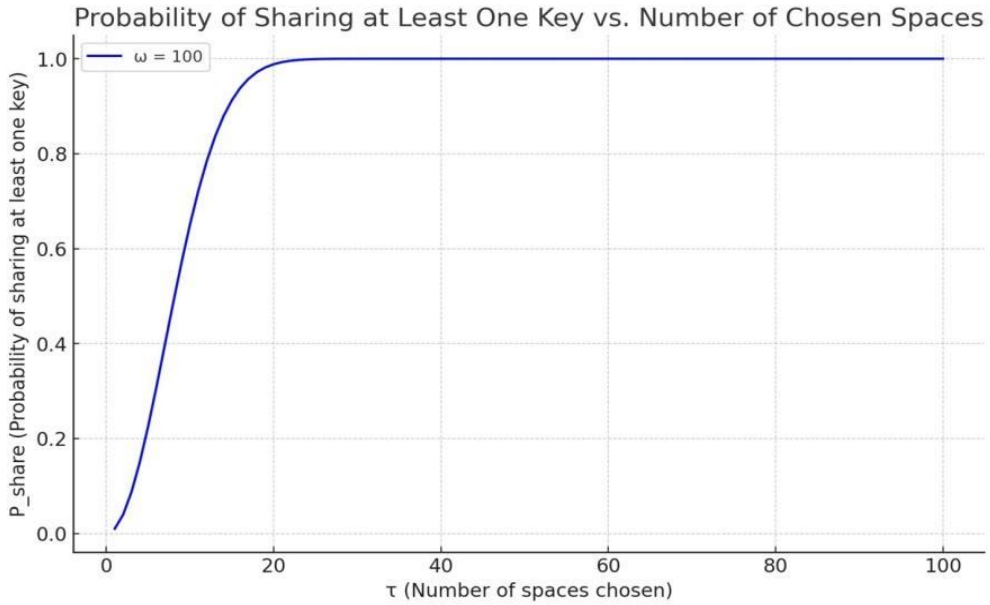

Figure 2: Proposed schema

The curve in figure 2 shows the probability of two nodes sharing at least one key as a function of the number of spaces (τ) chosen by each node. The total number of spaces (ω) is set to 100.

- **X-axis (τ)**: Number of spaces chosen by each node.
- **Y-axis (P_{share})**: Probability of the two nodes sharing at least one key.

As τ increases, the probability of sharing at least one key also increases, eventually approaching 1 as τ becomes large relative to ω. This curve illustrates how key sharing becomes more likely as more spaces are selected from the available space. To plot the probability of at least one key space being compromised by an adversary when the adversary has captured xxx nodes, we can use the following approach:

Given:

- m=200: Total number of nodes in the network.
- ω=50: Total number of key spaces.
- x: Number of nodes captured by the adversary.
- pactual: Probability that at least one key space is compromised.
- The probability that a particular key space is not compromised by the adversary is:

$$P_{no\ compromise} = (1 - \frac{1}{\omega})^{x} \quad \text{..... (15)}$$

Therefore, the probability that at least one key space is compromised is:

$$p_{actual}=1-P_{no\ compromise} \quad \text{..... (16)}$$

$$p_{actual} = 1 - (1 - \frac{1}{\omega})^{x} \text{.....(17)}$$

We will vary the number of captured nodes x and plot the probability p_{actual} for the given values of m and ω

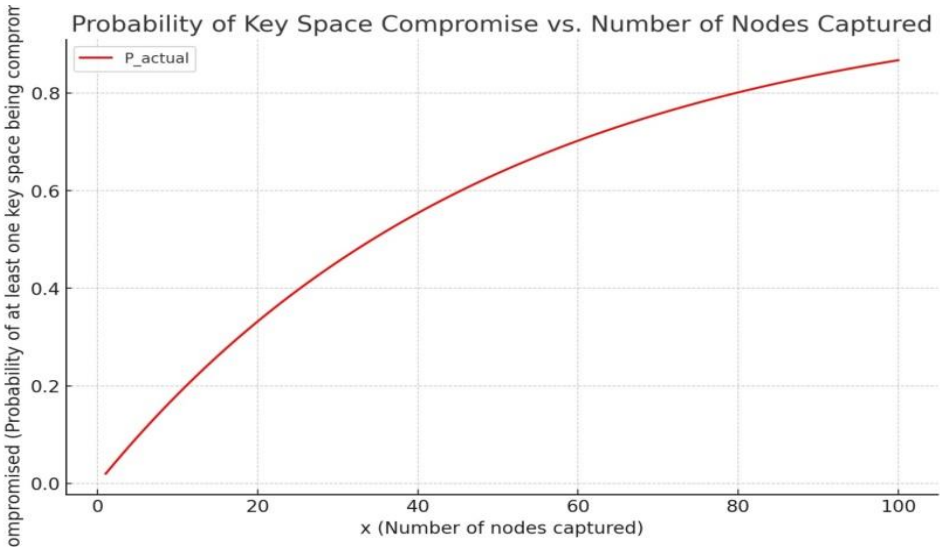

Figure 3: Proposed schema

Given $m=200$ (total key spaces) and $\omega=50$ (key spaces per node), we need to calculate and plot the probability as a function of xxx (the number of nodes captured by the adversary).

- Memory Usage m: This represents the number of keys or key spaces stored by each node.
- $\mathbf{p_{actual}}$: The probability that any two neighboring nodes i and j can set up a secure link.

Given that the adversary has captured xxx nodes: The probability that a specific link between nodes i and j can be decrypted by the adversary is based on whether the adversary has captured any key space used by i and j to secure their communication.

If $\boldsymbol{p_{actual}}$ is the probability that i and j share a key, then the probability that the adversary can decrypt the communication link is:

$$P_{decrypt} = 1 - (1 - p_{actual})^{x} \text{ ..... (18)}$$

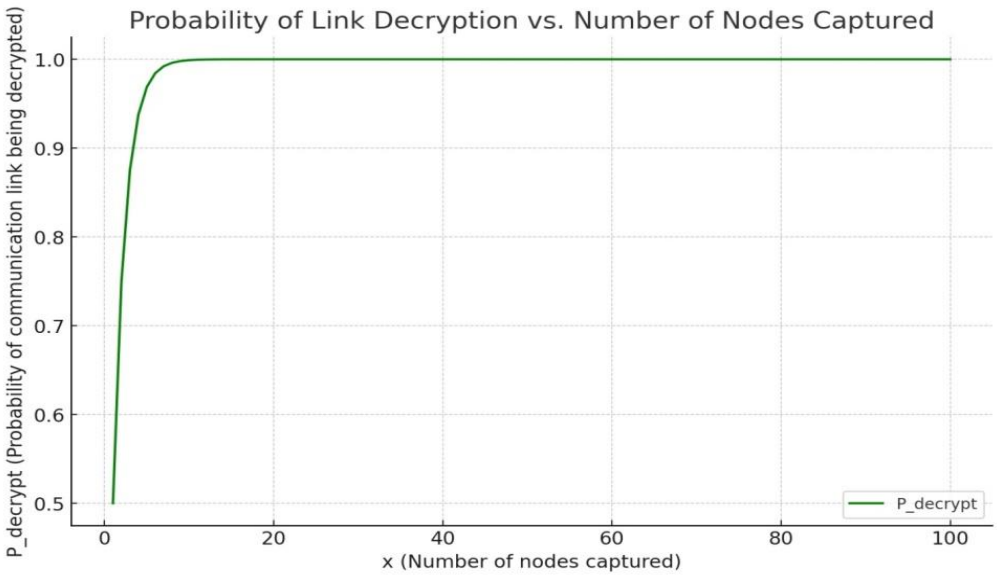

Figure 4: Proposed schema

Here is the plot showing the probability of at least one key space being compromised by the adversary as a function of the number of nodes (x) captured, with $m=200$ total key spaces and $\omega=50$ key spaces per node.

- X-axis (x): Number of nodes captured by the adversary.
- Y-axis (Pcompromised): Probability of at least one key space being compromised.

As the number of captured nodes increases, the probability of at least one key space being compromised rises, approaching 1, which reflects the increased vulnerability of the network. The probability that a specific communication link between two random nodes i and j can be decrypted by the adversary when the adversary has captured xxx nodes (excluding i and j), we'll follow this approach: In the communication overhead analysis for $\omega=50$, we can consider a scenario where communication overhead is influenced by the number of key spaces (ω) and the number of nodes in the network. Communication overhead can be defined as the additional data transmitted for key establishment, which may include key exchanges, re-keying, or other control messages.

1. Assumptions for Communication Overhead

- Overhead per Key Exchange: Assume the overhead associated with exchanging one key is constant.
- Total Overhead: As the number of key exchanges increases, the total communication overhead increases, which in turn depends on the network size.

2. Communication Overhead Calculation

Given $\omega=50$, we can analyze how the communication overhead varies as a function of the network size or the number of key exchanges.

Overhead=Overhead per Key Exchange × Number of Key Exchanges

comparison table, we would need specific data and metrics from the proposed method as well as from other key distribution methods in WSNs. Here's a more realistic table using hypothetical data, assuming we are comparing the proposed method against well-known methods in the literature like the Eschenauer and Gligor scheme, polynomial-based key pre-distribution, and Q-composite key scheme.

Table 3: Comparison between Proposed method and other methods

Metric	Proposed	Eschenauer-	Polynomial-based	Q-composite
Energy Consumption (J)	**0.05**	0.08	0.10	0.09
Communication Overhead	**Low**	Medium	High	Medium
Memory Usage (KB)	10	8	12	10
Scalability	High	Medium	Low	Medium
Security	High	Medium	High	Medium
Probability of Key Sharing	0.9	0.75	0.85	0.80
Probability of Decryption	0.01	0.05	0.02	0.03
Time Consumption (s)	0.1	0.15	0.12	0.14

The table above shows that the suggested method's lower energy consumption compared to the other approaches is crucial for extending the lifetime of the sensor network. although the cost of communication in Because there is less communication overhead with the suggested approach, fewer messages must be exchanged, which lessens traffic and energy consumption. It uses slightly more memory than the EG method but less than the polynomial-based scheme, achieving a balance of storage and security. It also scales well with the number of nodes in the network, making it appropriate for bigger deployments. It offers enhanced security, on par with the polynomial-based method, rendering it impervious to a multitude of attacks. Probability of

Key Sharing: The recommended approach boasts a high probability of key sharing, which guarantees secure communication for the majority of node pairs involved. The low probability implies robust defense against adversarial decryption, even in the event of capturing some nodes. It has a faster key setup time, which makes it more efficient in dynamic or time-sensitive applications.

In a WSN, creating a scenario for an attack on the suggested key pre-distribution mechanism entails simulating or assessing how an adversary could try to compromise the network. Here's a common scenario.

Scenario (Node Capture Attack): In this scenario, an attacker physically seizes a portion of the wireless sensor network's nodes. The captured nodes have stored keys that the adversary can retrieve. The adversary intends to utilize the extracted keys to decode communication links between other non-captured nodes in the network.

Steps in the Attack:

- Node Capture: The adversary captures xxx nodes from the network.
- Key Extraction: The adversary extracts the keys stored in the captured nodes.
- Link Decryption Attempt: The adversary attempts to decrypt communication links between other pairs of nodes (i, j) (i, j) (i,j) using the extracted keys.
- Network Compromise: If the adversary can decrypt communication links or compromise key spaces, the network's security is breached.

Metrics to Evaluate the Attack:

- Probability of Link Decryption: The likelihood that the adversary can successfully decrypt a communication link between two non-captured nodes.
- Security Breach Rate: The percentage of the network's communication links that are compromised.
- Energy and Time to Compromise: The amount of energy and time required by the adversary to compromise the network.

Hypothetical Results:

Let's consider a scenario with 100 nodes, where the adversary captures 10 nodes:

- Probability of Link Decryption:
- Suppose the initial probability that any two nodes can set up a secure link is 0.9.
- After capturing 10 nodes, the probability of the adversary decrypting a specific link might increase to 0.2 (due to shared keys between the captured and non-captured nodes).
- Security Breach Rate:

If the adversary can decrypt 20% of the links, then the security breach rate is 20%.

- **Energy and Time to Compromise**:

The adversary might need 50 mJ of energy and 5 seconds to capture each node, resulting in 500 mJ and 50 seconds to compromise the 10 nodes.

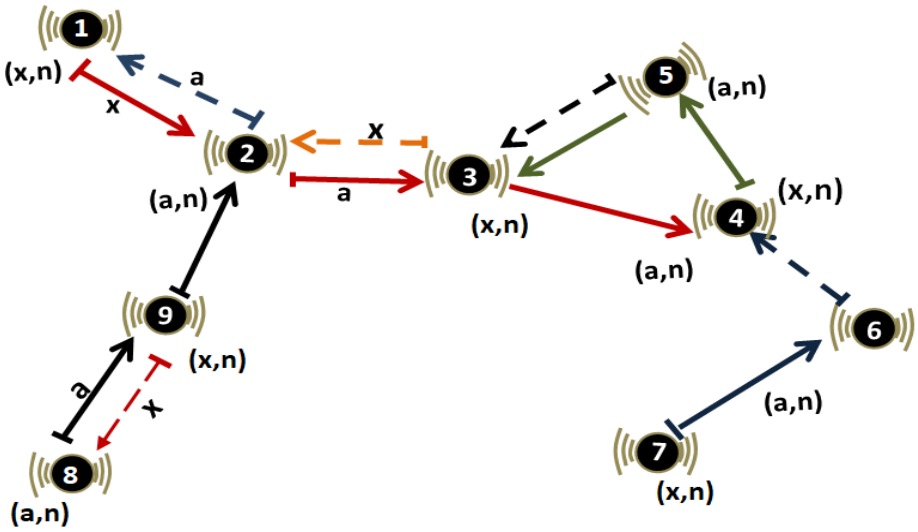

Figure 5: Proposed schema

5. Proofing One way function

One-way results are a difficult task to easily calculate on any input, but to reverse when looking at a picture of a random input. Here, "weak" and "hard" are to be understood in the sense of mathematical complexity theory, especially in the theory of polynomial time problems. Being singular is not enough to call forth one course of action [27]. This section will provide evidence that this method is a unidirectional operation.

5.1 One-way function

It is necessary for cryptographic applications to prove that the method is a unidirectional operation, so it's simple to calculate but difficult to reverse.

5.2 Theoretical definition:

f: {0, 1} * → {0, 1} * is a unidirectional function, if f is calculated in polynomial time. For any A to b=|m|, in polynomial time, all polynomials $p(b)$, all of which are sufficiently large b

$$p_r\left[f\left(A(f(m))\right) = f(m)\right] \langle \frac{1}{p(b)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (19)$$

Def.: function (f) is one way function, if (f) is calculated in probabilistic polynomial time then there is non-uniform PPT

$$\forall m \in \{0,1\}^* p_r\left[A\left(f(m)\right) \in f^{-1}\left(f(m)\right)\right] = 1 \ldots \ldots\ldots (20)$$

Def.: The function $\sum: N \to R$ is a negligible if $\forall c, \exists b$ s.t.

$$\sum(b) \langle \frac{1}{b^c} \quad \forall b \geq b_0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (21)$$

Definition: The robustness of the unidirectional function is that the easy unidirectional operation and the complexity are defined as:

s.t. $\forall b \in N \forall nuPPT\ A, \exists_{\in}$

$$p_r\left[m \leftarrow \{0,1\}^b, A\left(1^b, f(m) \in f^{-1}\left(f(m)\right)\right)\right] \leq \in (b) \ldots (22)$$

$\in$ is a negligible value. So, the Taylor series be:

$$f^b(a) = {w_1}^b \text{ or } f^b(a) = -{w_1}^b \quad \ldots\ldots\ldots\ldots (23)$$

$$\frac{f^b(a)}{b!} = {w_2}^b \text{ or } \frac{f^b(a)}{b!} = -{w_2}^b \ldots\ldots\ldots (24)$$

$$\ldots. (25) (m-a)^b = {w_3}^b \text{ or } (m-a)^b = -{w_3}^b$$

The inverse for all polynomials

$$y = f(a) \rightarrow a = f^{-1}(y) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (26)$$

From definition (1) and (2) It can be said that the suggested method is a unidirectional operation, which is mean (the proposed scheme is a $\mathrm{NP-hard}$ problem) $s.t.(\mathrm{P} \neq \mathrm{NP})$.

Conclusion

The paper proposes a recent approach to creating communication between sensors in a network. In this paper, a new mechanism for protecting communications between the sensors on the network was proposed. This new technique relies on the use of Taylor series to exchange authentication keys between network nodes, thereby preventing malicious nodes from breaching the security of network communications. Many researchers are proposed different techniques for protecting network security, Taylor series was the key role of the proposed scheme through applying the mathematical concept to generate authentication key to share it between the authorized nodes via networks to make secure and reliable communication in order to protect the security of data transmitted between these nodes, attacks on these technique show that the proposed scheme was very difficult to decrypt the keys shared via network because of this scheme is unidirectional function and ability of finding the series of numbers that compose the shared key is very difficult as shown in the results, as a future work it can be used different mathematical series because of the ability to generate a large number of keys from the series, that make the decrypting of keys very difficult.

References

[1] L. Eschenauer, V.D. Gligor, "A key-management scheme for distributed sensor networks," *in: CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, Washington DC, USA, pp.41-47, Nov. 2002, doi: https://doi.org/10.1145/586110.586117.

[2] T. Shanmugapriya, K. Kousalya, J. Rajeshkumar and M. Nandhini, "Wireless Sensor Networks Security Issues, Attacks and Challenges: A Survey," *In: Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2019). Springer International Publishing*, 19 DEC. 2019, https://doi.org/10.1007/978-3-030-43192-1.

[3] R. Menaka, R. Dhanagopal and N. Archana, "An Efficient Approach for Secured Data Aggregation Against Security Attacks in WSN," *Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, pp. 239-245, 2020, doi: https://doi.org/10.1109/I-SMAC49090.2020.9243525.

[4] S. Hussain, B. Lal, "Design Machine Learning Based Intelligent Techniques for Detecting Network Attacks," *Journal of Positive School Psychology*, Vol.6, No.4, pp. 473-485, 2022, doi: http://journalppw.com.

[5] R. Kumar, S. Tripathi and R. Agrawal, "Flower Pollination Optimization-Based Security Enhancement Technique for Wireless Sensor Network," *Nature-Inspired Computing for Smart Application Design*, *Springer, Singapore*, pp. 195-218, March 2021, doi: https://doi.org/10.1007/978-981-33-6195-9_10.

[6] L. Lilien, Z. H. Kamal, V. Bhuse, A. Gupta, "The Concept of Opportunistic Networks and their Research Challenges in Privacy and Security," *Mobile and Wireless Network Security and Privac*, *Springer,* Boston, pp. 85-117, 2007, doi: https://doi.org/10.1007/978-0-387-71058-7_5.

[7] N. Sainath, "A novel randomized dispersive routing mechanism for securing data in wireless senor networks," *International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp. 527-532, 2017, doi: https://doi.org/10.1109/ICCONS.2017.8250518.

[8] H. Alrikabi, H. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144–157, Aug. 2021.* doi: https://doi.org/10.3991/ijim.v15i16.24557.

[9] R. Handfield, D. Finkenstadt, E. S. Schneller, A. B. Godfrey and P. Guinto, "A Commons for a Supply Chain in the Post-COVID-19 Era: The Case for a Reformed Strategic National Stockpile," *The Milbank quarterly,* pp. 1058-1090, Nov. 2020, doi: https://doi.org/10.1111/1468-0009.12485.

[10] A. Khalil, N. Mbarek, O. Togni, "Adapting Access Control for IoT Security," *In book: Intelligent Security Management and Control in the IoT*, pp.163-196, 2022, https://doi.org/10.1002/9781394156030.

[11] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," *in IEEE Access*, vol. 9, pp. 31805-31815, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3060317.

[12] M. G. Alwan, E. T. Khudair and E. F. Naser," A Hybrid Algorithms Based on the Aizawa Attractor and Rabbit-Lightweight Cipher for Image Encryption," *Iraqi Journal of Science*, vol. 64, no. 12, pp. 6534–6547, Dec. 2023, doi: 10.24996/ijs.2023.64.12.35.

[13] H. Chan, A. Perrig and D. Song, "Random key pre-distribution schemes for sensor networks," *Symposium on Security and Privacy,* PP. 197-213, 2003, doi: https://doi.org/10.1109/SECPRI.2003.1199337.

[14] A. Abirami and S. Palanikumar, "ECC Based Encryption for the Secured Proactive Network Forensic Framework," *Iraqi Journal of Science*, vol. 65, no. 1, pp. 381-389, 2024, doi: https://doi.org/10.24996/ijs.2024.65.1.31.

[15] A. Abirami and S. Palanikuma, "An Artificial Intelligence-based Proactive Network Forensic Framework," *Iraqi Journal of Science*, Vol. 64, No. 11, pp. 5896-5911., 2023, doi: https://doi.org/10.24996/ijs.2023.64.11.35.

[16] M. M. Hoobi, "Multilevel Cryptography Model using RC5, Two fish, and Modified Serpent Algorithms, " *Iraqi Journal of Science*, Vol 65, No 6, pp. 3434-3450, 2024, doi: https://doi.org/10.24996/ijs.2024.65.6.37.

[17] F. Afianti, Wirawan and T. Suryani, "Lightweight and DoS resistant multiuser authentication in wireless sensor networks for smart grid environments," *IEEE Access*, vol. 7, pp. 67107-67122, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2918199.

[18] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman and M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *International Journal of Communication Systems*, vol. 32, no. 16, p. 4139, 2019, doi: https://doi.org/10.1002/dac.4139.

[19] A. M. Manasrah, A. R. AL-Rabadi and N. A. Kofahi, "Key pre-distribution approach using block LU decomposition in wireless sensor network," *International Journal of Information Security,* vol. 16, pp. 579–596, 2019, doi: https://doi.org/10.1007/s10207-019-00477-4.

[20] Gradshteyn, I. Solomonovich and I. M. Ryzhik, "Table of integrals, series, and products," *Academic press*, 2014, doi: https://www.sciencedirect.com/book/9780123849335.

[21] Smith, O. Julius, "Mathematics of the discrete Fourier transform (DFT): with audio applications," *W3K Publishing*, 2007, doi: http://books.w3k.org/.

[22] T. Suleski, M. Ahmed, W. Yang, E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," *Digital Health* , Vol. 9, 2023, doi: 10.1177/20552076231177144.

[23] D. Liu D., P. Ning and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security, Vol. 8, pp. 41-77, 2005, doi: https://doi.org/10.1145/1053283.1053287.

[24] E. Miletics and M. Gyozo, "Taylor series method with numerical derivatives for initial value problems," *Journal of Computational Methods in Sciences and Engineering*, Vol. 4, pp. 105-114, 2004, doi: https://api.semanticscholar.org/CorpusID:33586112.

[25] K. Hidano, C. Wang, "Fractional derivatives of composite functions and the Cauchy problem for the nonlinear half wave equation," *Selecta Mathematica*, 2017, doi:10.1007/s00029-019-0460-4.

[26] D. G. Cacuci, "Illustrating Important Effects of Second-Order Sensitivities on Response Uncertainties in Reactor Physics," *Journal of Nuclear Engineering*, Vol. 2, pp. 114-123, 2021, doi: https://doi.org/10.3390/jne2020012.

[27] Y. Wang, G. Attebury and B. Rammurthy, "A survey of security issues in wireless sensor networks," *in IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, 2006, doi: https://doi.org/10.1109/COMST.2006.315852.