IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 1, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Sinkhole Detection in A Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption

Dr.S.Sumathi[1], T. Lavanya[2]

Professor & Head, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Krishnagiri, Tamil Nadu, India[1]

P.G Scholar, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Krishnagiri, Tamil Nadu, India[2]

ABSTRACT: In a wireless sensor network , the sensors regularly communicate sensed data from a specified environment to a centralized station using wireless communication. In an open environment, deployment increases the risk of security assaults. When a sinkhole node advertises itself as the best route to the base station, it draws other nodes to the area and launches a damaging attack against the network layer. Subsequently obtaining packets from additional sensor nodes and jeo pardising network security. In order to guarantee data integrity during transmission, this work provides a simple, safe mechanism based on the Threshold Sensitive Energy Efficient Sensor Network protocol and watermarking techniques. This approach uses homomorphic encryption to enable quick and effective sensor node identification that uses less energy. The reason for finding and stopping sinkholes. The findings demonstrate that by identifying the sinkhole attacker node before the attack is launched, the suggested technique improves security.

KEYWORDS: Clustered protocol, TEEN protocol, watermarking, wireless sensor network, security,sinkhole attack.

I. INTRODUCTION

Because they may be improved upon and overcome the limitations of older types of networks, Wireless Sensor Networks (WSNs) have encroached onto numerous industries (such as industry, ecology, agriculture, and infrastructure) [1]. They are made out of tiny, inexpensive sensor nodes that can sense their surroundings, which accounts for their flexibility[2]. These nodes are often quite small and dispersed around a region to gather information. They are accompanied by a stronger Base Station (BS) or sink node[3]. These nodes do, however, have some design limitations, including short battery life, little memory, and constrained computational and processing power[1]. As a result, these constraints present difficulties for various application requirement designs, including security.

Security must be established as one of the essential criteria for a variety of WSN applications. WSNs are prone to a variety of security assaults since they are typically installed in hostile environments [4]. Moreover, as all nodes communicate their data to the BS in WSNs using the many-to-one communication pattern, additional vulnerabilities are added [5]. Because of this, WSNs are vulnerable to both insider and outsider attacks. When an external entity is introduced into the network with the intention of compromising network functionality, an outsider attack occurs[6]. Insider attacks occur.

A serious insider assault known as a sinkhole or black hole is classified as an active routing disruption attack on the network layer[8]. By promoting itself as a high-quality routing path to the BS (closer to the BS than other nodes), the attacker node draws additional nodes in this type of attack[9]. As a result, nodes regularly employ the malicious node path, which has the ability to alter, spoof, or drop transmitted packets [10]. Even though public key and private key cryptography are successfully used to protect data integrity and guarantee authentication in many different types of networks, they cannot be implemented in WSNs because they require more computational power and drain the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

energy of the nodes, which shortens the network's lifetime [3]. Thus, suggestions for securing WSNs should make use of approaches. Consequently, ideas for securing WSNs should apply strategies that do not affect the networks longevity.

Several methods for the detection of suspicious nodes have been presented by various researchers; they are discussed in more detail in Part II below. Some works employ predetermined rule sets, while others count the amount of hops from the node to the BS. While some studies set a trustworthiness criterion and utilize it to examine each node in the network, other ways are based on mobile agents. Although many of these works success totally detected the sinkhole attack, however many of them suffer for the incapability to detect the manipulation on the data or detecting more than one attacker node at a time. Moreover, neither the message replaying attack nor the injection attack can be detected activated by the sinkhole attacker more computational capability which cannot be WSNs.

The suggested work uses watermarking as a benefit to safeguard sensed data during transmission. Homomorphic encryption is employed for intercommunication, and a network key is used to identify the sink hole node. The study's contributions include. In Part III, the system model that was employed for this work is discussed and demonstrated. In Section IV, a demonstration of the suggested plan is provided. The suggested work's security analysis is presented in Section V. The experimental design and evaluation findings are presented in Section VI. Section VII also outlines the conclusion and future work.

II. RELATED WORKS

2.1 Work Based on Trust

Using sinkhole message delay in the hierarchal WSNs as an example, Wazid et al. [5] proposed a detection system which is capable of handling the three types of sinkhole attacks (HWSN). Each cluster in their HWSN is divided into two node categories: high-end nodes and other nodes. High-end nodes are in charge of keeping an eye on the cluster and seeing any unusual behaviour that would point to a sinkhole assault. Such secure systems produce adequate results, but they have substantial energy and message overhead, which makes them less suitable for WSNs.

2.2 Works with Mobile Agents

Hamed Heidari and Rafeh [7] suggested a mobile agent based system that can roam between nodes and is self-regulating (from anode to a one-hop neighbor). Their primary strategy for identifying the attacker is to employ the principle of agent cycling, which means that during each time of inactivity, the agent cycles over all of its immediate neighbours. After the cycle is complete, if the agent does not return to its original node within a predetermined length of time, the cycle will be repeated once more for assurance. If the agent does not return to the node after two tries, the node is taken into consideration.

2.3 Work Based on Probabilities

The ASA algorithm was developed by Jahandoust and Ghassemi [8] and runs in AODV ver12.2 using subjective logic and the probabilistic extension of timed automata to identify the attacked node. In their work, a routing database is kept that makes use of probabilistic data to generate an opinion about each network node. Each node is monitored by a distributed node, and the routing table records the dynamic changes in the routing path as a result of those changes. Their work's key drawback is that it necessitates excessive computing, which uses up nodes' energy and shortens the network lifetime.

III. EXISTING METHOD

To detect and prevent sinkhole attacks based on the residual energy paired with the trustworth value of each node, each region is first examined using a geo statistical hazard technique. Second, a migration scheme modifies the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

routing path to exclude any paths impacted by the assault, thwarting it and removing its impact on the network. The key drawback of a system like this, which divides the network into regions based on the amount of energy spent, is that some parts have higher congestion rates, which reduce the system's ability to detect sinkhole attacks.

Hanetal.[9] divided sensor nodes into two categories: event nodes and intermediate nodes. An event node is an angle sensor node that gathers data and sends it to the base station. Between the sensor node and sink node, an intermediate node is in charge of routing and data transfer. Their suggested technique (IDASA) employs three phases for the detection and eradication of intruders. The first stage in route research is to retrieve the shortest and longest paths between nodes, with the middle node in the shortest path being considered to be a malicious node. Second, a determination is made regarding that node based on ACK signals and interaction times. The event node decides and eliminates a suspicious node in the last stage. Although their work has a high sinkhole detection rate, energy use is also substantial because it is necessary to investigate every possible route for a sinkhole attack.

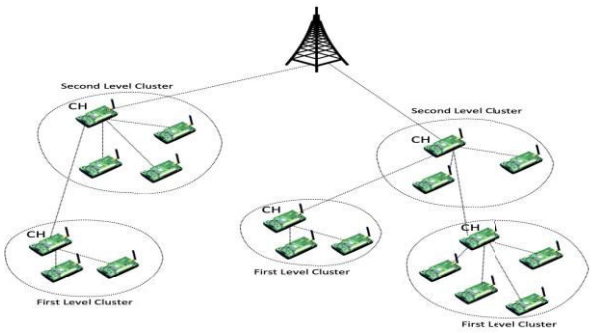

Fig 1. Clustered Network

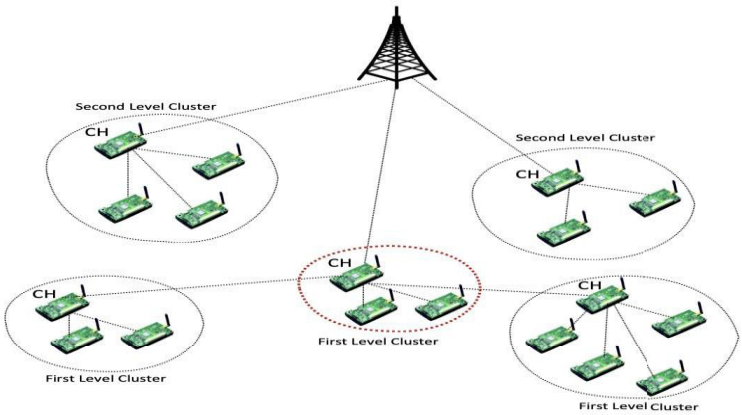

Fig 2. Sinkhole attack in a Network

IV. PROPOSED SYSTEM

This section outlines the suggested method, which employs homomorphic encryption to identify and thwart sinkhole attacks as well as watermarking techniques to guarantee the data's authenticity and integrity during transmission. We go into further depth about the suggested technique in the following section.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

4.1 Initialization Phase

First process in the initialization phase is the key generation process. In the proposed work, the BS is in charge of generating two distinct keys: the network key and the cluster key. Network key is used to encrypt and decrypt the nodes ID during communication across clusters. Authentication of the data and tamper detection are ensured by the cluster key, which is used for communication within the cluster and for data transmission from the cluster member to the cluster head. These two keys were created using the quick Paillier cryptosystem which proved to be fast and require few computational powers. The network creates various tiers of clusters, each with a CH, using the TEEN protocol. The BS encrypts sensor node IDs after cluster creation before sending them to the CHs. The BS uses a homomorphic private-key encryption system with the network key (Kn) produced in the BS to stop an attacker node from changing its key. Homomorphic encryption is a highly lightweight encryption method that may be employed in WSN without compromising network life time, unlike other encryption algorithms, which are typically expensive and difficult to compute [3]. Moreover, homomorphic encryption makes it simple to combine IDs into data while maintaining data property.

$$C = Enc(d, k, M) = d + k \bmod M$$

where k is the network key (Kn), M is the modulus, and d is the message that has to be encrypted. The sensor nodes are given identifiers by the BS to specify which cluster they adhere to and at what level.

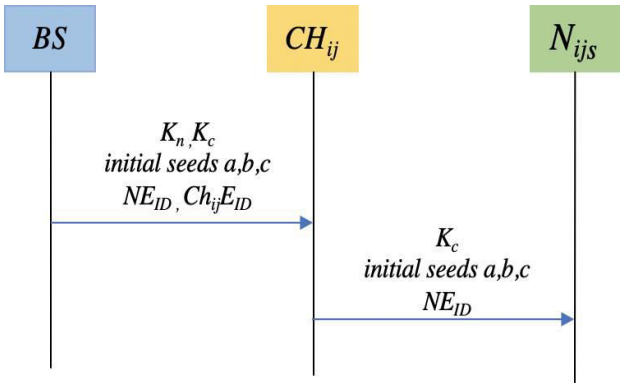

Fig 3. Initialization Phase

4.2 Sensing Phase

To ensure the ownership of the sensed data at this phase, the sensor nodes employ a watermarking mechanism. A watermark is a piece of information that is applied to data to prevent copying or modification while maintaining the functionality of the data [1]. This gives the data security and copyright [4]. Creating a watermark for a data packet does not require storage or extra processing which is particularly ideal to use in WSN. Including a digital watermark guarantees the integrity and secrecy of the data.

The key used in this proposal's keyed hash functions is the Keyc, which is distributed to the sensor nodes inside each cluster. The proposed work uses watermarking based on PRNG to ensure the randomness of the watermarking bytes positions along with HMAC to benefit from the strength of the generated bytes while maintaining the ability to reproduce the same bytes in the exact positions for the comparison process to authenticate the sensor nodes, in contrast to other authentication schemes that only rely on HMAC.To prevent the nodes in the cluster from reporting sensingdata more than one time, each node places a *Time Stamp* on a packet before reporting it to the CH, as shown in Fig.4. Proposed watermarking scheme is shown in Fig. 5 and uses Algorithm l.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

V. BLOCK DIAGRAM

In this work, water marking is accomplished by injecting one byte into each of the two locations (P1, P2) that the pseudo-random number generator chose at random (PRNG). A better level of security is provided by using PRNG, which guarantees a high amount of unpredictability. A cryptographic message digest or hash-based message authentication code (HMAC), which converts data of variable length to data of fixed length, creates the content of these two bytes. Because of the high security level of this function, malevolent users cannot deduce the message's pre-image from its hash value. These qualities allow the hash function's output values to be used for auxiliary or integrity data checks. There are two types of hash operations: keyed hashes and un-keyed hashes

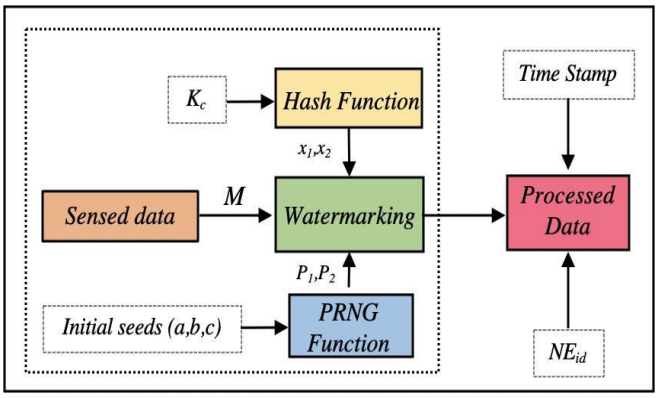

Fig 4. Sensor node Water marking scheme

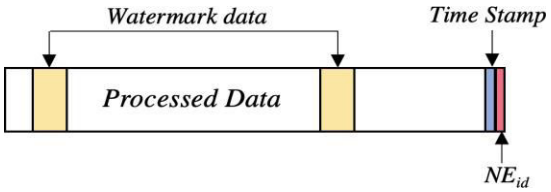

Fig 5. Processed content of the data

The TEEN protocol offers one level of security since it restricts communication between sensor nodes in various clusters; in other words, sensor nodes only report to their CH. According to this suggestion, all communications between sensors in various clusters must go through respective CHs in order to verify the identity of the nodes.

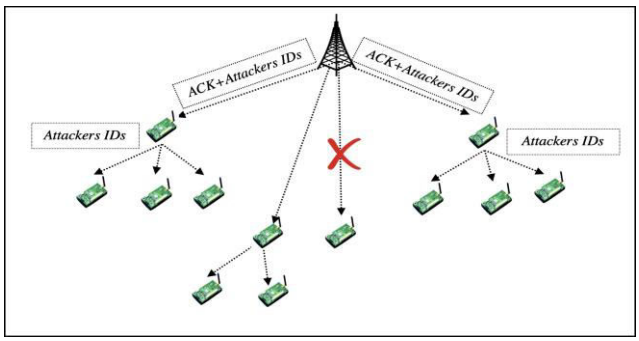

Fig 6 .Cluster head attack detection and cluster reformation

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

VI. EXPERIMENTAL RESULTS

The throughput results for the two networks are shown in Fig. 7, where the y-axis displays the throughput numbers and the x-axis the number of network nodes (in Kbps). Figure 8 shows that as the the network's transmission rate rises along with the number of sensor nodes, throughput values likewise rise. Since the sinkhole node drops incoming packets, lowering throughput values, all packets are successfully delivered in the secured TEEN network, resulting in higher throughput values across all network sizes, the throughput values of the secured TEEN are higher than the values of the TEEN under attack. Whereas [6] has a throughput value of 99 (Kbps), the suggested work has a throughput value of 150. (Kbps). The delay findings (in seconds) are shown in Fig. 8, which amply reveals that the network being attacked has a very high value for the delay induced by re-transmissions brought on by the sinkhole attack node. In contrast, considering the security mechanisms put in place to aid in the safe transmission of all packets, the delay values for the secure TEEN are quite low for all network sizes (10, 50, and 100).

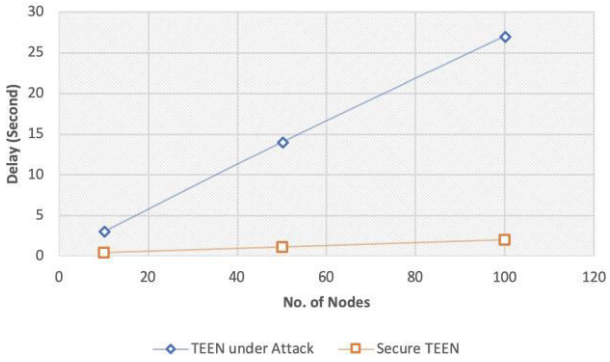

Fig 7. Reduced delay

Results for energy usage are shown in Fig. 8. Because to the use of the watermarking approach, node authentication in the CHs and BS, and the use of homomorphic cryptography to authenticate the sender node in the communication processes, the secured TEEN network requires more network energy than the network that is under assault. The messages used in the proposed work here to inform the nodes to any attacks and alarm messages from CH are another energy usage factor to BS if a sinkhole attack detected. Even if the network under attack uses less energy than the secured TEEN, this discrepancy is acceptable while assuring the network's security. The suggested study employs homomorphic cryptography exclusively for the IDs in addition to a less energy-intensive watermarking technique, in contrast to [9], where they employed homomorphic cryptography in CHs to encrypt all of the incoming sensed data from the sensor nodes.

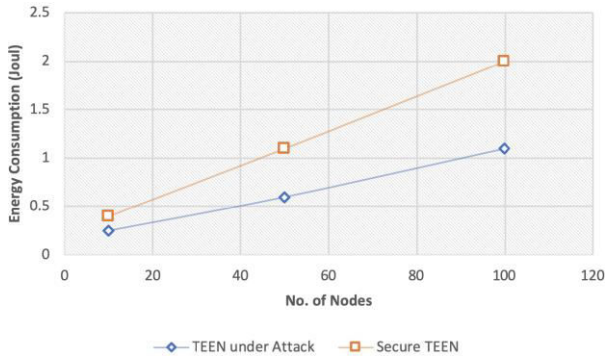

Fig 8. Energy Consumption result

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 12, Special Issue 1, April 2023
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

VII. FUTURE SCOPE

Our project focuses mainly on sinkhole attacks and proposes a technique to isolate those attacks in WSN, In future these can be extended to detect and resolve Sybil attacks, jamming or packet injection attacks, wormhole attacks of the WSNs.

VIII. CONCLUSION

Using homomorphic encryption and watermarking methods, we provide a secure sinkhole detection and transmission model in this study. The suggested method relies on two major communication techniques found in the TEEN protocol. Each time the cluster configuration varies, the BS generates and distributes a new version of these forms. We add watermarks to every data packet to secure data authentication. These watermarks are generated via a pseudo-random number generator and the message authentication algorithm. The usage of the encrypted IDs of the sensor nodes using homomorphic encryption is another security mechanism used to secure the identity of the sensor nodes in communications between nodes from different clusters. This strategy has secured funding with zero failures**.**

REFERENCES

[1] T. Kaur and D. Kumar, ‘‘A survey on QoS mechanisms in WSN for com- putational intelligence based routing protocols,’’ *Wireless Netw.*, vol. 26, no. 4, pp. 2465–2486, May 2020

[2] I. Tomic and J. A. McCann, ‘‘A survey of potential security issues in existing wireless sensor network protocols,’’ *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.

[3] J. Louw, G. Niezen, T. D. Ramotsoela, and A. M. Abu-Mahfouz, ‘‘A key distribution scheme using elliptic curve cryptography in wireless sensor networks,’’ in *Proc. IEEE 14th Int. Conf. Ind. Informat. (INDIN)*, Jul. 2016, pp. 1166–1170.

[4] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detec- tion system,’’ *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–13, Jan. 2019.

[5] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, ‘‘Design of sinkhole node detection mechanism for hierarchical wireless sensor networks,’’ *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4596–4614, Nov. 2016.

[6] N. Nithiyanandam and P. Latha, ‘‘Artificial bee colony based sinkhole detection in wireless sensor networks,’’ *J. Ambient Intell. Humanized Comput.*, vol. 7889, pp. 1–14, Jul. 2019.

[7] Z. Zhang, S. Liu, Y. Bai, and Y. Zheng, ‘‘M optimal routes hops strategy: Detecting sinkhole attacks in wireless sensor networks,’’ *Cluster Comput.*, vol. 22, no. 3, pp. 7677–7685, May 2019.

[8] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, ‘‘A secure data rout- ing schema for WSN using elliptic curve cryptography and homomor- phic encryption,’’ *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 28, no. 3, pp. 262–275, Jul. 2016.

[9] X. Liu, A. Liu, T. Wang, K. Ota, M. Dong, Y. Liu, and Z. Cai, ‘‘Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks,’’ *J. Parallel Distrib. Comput.*, vol. 135, pp. 140–155, Jan. 2020.

[10] M. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. Abdel-Rahman, ‘‘Game theory meets wireless sensor networks security requirements and threats mitigation: A survey,’’ *Sensors*, vol. 16, no. 7, p. 1003, 2016.

[11] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking," in IEEE Access, vol. 8, pp. 92098-92109, 2020, doi: 10.1109/ACCESS.2020.2994587.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization *Volume 12, Special Issue 1, April 2023*
10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)
5th -6th April 2023
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Biography

Dr. S. Sumathi,
Professor,
Department of Electronics and Communication Engineering,
Adhiyamaan college of Engineering(Autonomous),
Hosur.

Lavanya. T, PG Scholar,
M.E. Communication Syatems, Adhiyamaan college of Engineering(Autonomous),
Hosur.

INNO SPACE
SJIF Scientific Journal Impact Factor

SJIF: 8.423

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details