The Survey of Various Security Schemes of Wireless Sensor Networks

Md Ajaz Rab[1], Dr. Jameel Ahmad[2]

[1]Research Scholar, Department of CSE, Integral University, Lucknow

[2]Assistant Professor, Department of CSE, Integral University, Lucknow

Abstract - A network that does not contain any central controller within it and is self-configuring in nature is known as a wireless sensor network. It is difficult to maintain the security and energy consumption of these networks due to such properties. When any kinds of malicious nodes enter the network, a scenario of attack occurs in that network. There are several types attacks found in the network which are all categorized into active and passive types depending upon the manner in which they attack. The various schemes are designed to improve security of wireless sensor networks. The designed techniques are reviewed in terms of methodology and performance.

Keywords - WSN, Security Attacks, Thrust mechanism, PLC, RTU

I. INTRODUCTION

A wireless sensor network (WSN) can be defined as a group of sensor nodes with finite resources that achieve a common purpose by working in coordination. Typically, the main functions of sensors include sensing and monitoring their area of deployment, collecting sensor information from the environment, processing data, and communicating with other devices [1]. Sensor nodes are deemed as one of the three main constituents that are included in the deployment framework in a WSN, which are: (1) sensor nodes, (2) radio co-ordinators, and (3) a programmable logic controller (PLC) or any human-computer interface (HCI) backing up a Remote Terminal Unit (RTU). Sensor nodes can have faults and due to their exposure on the web, they can become unreliable in no time and anyone gets physical access to them for free. A typical sensor consists of four basic units: a power source, a radio, a processor, and an actuator. At the other side, they have many limitations with respect to energy, data transmission, computation and storing. It is possible to deploy thousands of such nodes in some target locations to collect data for upcoming purposes, such as meteorological purposes, smart homes etc [2].

1.1 Cybersecurity Attacks in Wireless Sensor Networks

The classification of cyber security attacks can be done in two general modes, which are: (a) passive attacks and (b) active attacks. Cyber security is the practice of providing security to networks, devices, and data from illegal accessibility. It is basically an art to ensure the data confidentiality, integrity and accessibility.

i. Passive attacks: The attackers activate passive attacks only to overhear communications (hence eavesdropping) and analyse the traffic shared without modifying the vulnerable system [3]. This attack variant is extremely perilous and complex to locate as it is performed silently without affecting the system. Consequently, the assailant aims to collect some private information simultaneously, as well as gain knowledge about expressive nodes in the network (cluster head nodes) to get ready for an active attack, which can be devastating.

ii. Active attacks: In active attacks, the adversary tries to delete or replace messages exchanged over the network. The assailant can do anything damaging if he has the potential to execute his purpose.

1.2 Security of WSN in Healthcare Sector

Wireless healthcare networks have brought revolution in the way of patient monitoring in the healthcare domain by presenting a more efficient substitute of the conventional way of managing patient health. Since every technology has some shortcomings along with advantages, the free-access characteristic of the network brings its confidentiality under question [4]. Illegal access actions and unrestricted threats can develop security issues for the healthcare data of the patient. The data gathered by the devices implanted on the patient’s body for healthcare monitoring may lead to security concerns. The exposure of sensor nodes to the internet increases their vulnerability to different variants of attacks, for example, distributed denial-of-service (DDoS) attack. This attack type is deemed as one of the major concerns as adversary can collapse the security of the network and can further activate a clone node attack, or a replication attack which is amongst the most threatening assaults. When the sensor node transferring the patient's sensitive health data is attacked, the attacks not only swap the sensor nodes with duplicates of the sensor nodes but also displace the real data with bogus data and install the sensor node on the database again. Wireless healthcare systems are available to everyone across the world, and have ensured their reach to every part of the globe [5]. The free-access characteristic of the technology of the wireless healthcare network and its wireless channels increases the insecurity of the data transmitted over the network.

1.2.1 Node Replication or clone Node Attack

The dynamic operational nature of WSNs make them often unrecoverable, therefore they are prone to a variety of new attacks. For example, an adversary can listen to all network communications. In addition, a malicious node can capture all the information stored therein by the receiving nodes. Sensors are generally not considered forgery-proof [6]. Since a clone contains valid information (code and cryptographic material), it can join in network operations in the similar fashion as a normal node; therefore, cloned nodes are able to active a vast range of attacks. For example, a clone can generate a black hole, launch a wormhole attack with an allied opponent, or insert false data or aggregate data so as to manipulate the ultimate result. In addition, clones can perform information leakage. The following two important points may help illustrate the severity of a clone attack [7]:

- A clone can pretend to be completely truthful to its surrounding nodes. Truthful nodes indeed may not be aware of the truth without global counterexamples that there is a clone among their surroundings.
- In order to have a vast number of colluded nodes [8], it is not required for an adversary to compromise a large number of nodes. In fact, upon acquiring and contaminating one node, the main cost of the attack persists. It may be considered cheaper to make more clones of the similar node.

1.2.2 Diagrammatic Representation of replication attack in WSN

A node replication attack or clone node attack is a security concern where an adversary reprograms or regenerates WSN sensor nodes and connects to the target network by pretending to be valid nodes of that specific network. Considering cost, these sensors tend to lack tamper resistance hardware [9]. Figure 1 shows a node replication attack in a WSN.

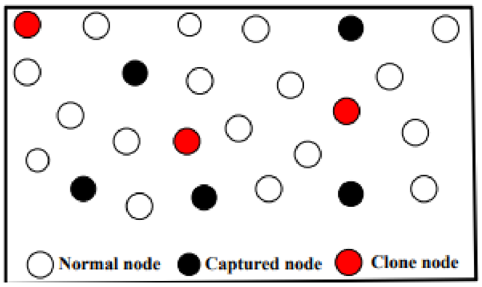

Fig. 1. A WSN with clone nodes

After the attacker has captured the honest node, all information is obtained from the honest node. The assailant then reinjects this acquired node into the network with no modifications. Typically, when an assailant activates a node replication attack, the duplicates are installed in the relevant and appropriate position in the WSN [10]. In a static wireless network, the nodes are immobile, which means that their location remains unchanged after deployment. However, the situation differs from that of mobile wireless sensor networks where the nodes are dynamic in nature, without any static location. From this viewpoint, it is clear that the methods adopted for detecting node replication attacks in static WSNs may be different from those of mobile WSNs [11].

1.3 Replication or Node Clone Detection Techniques in WSN

Clone attack is amongst the most important security attacks in sensor networks. After a sensor node is compromised, a malevolent user can install fake sensor nodes in WSNs to activate a rage of deceptive attacks. Therefore, tracing clone nodes in less cost is essential to guarantee the network security. Several clone detection protocols exist in the literature [12]. Generally speaking, clone detection protocols can be categorized into two classes, known as, centralized and distributed protocols:

a. Centralized clone detection protocol: Sensor nodes use a centralized clone detection protocol to transmit their privacy information to the base station, and the node at the base station determines the authenticity of the sensor node by making comparison of the privacy information to its already saved records. This kind of scheme has less communication overhead and intricacy. In the centralized clone detection protocol [13], malevolent users can listen to the communication between the sink node and the sensor nodes, and obtain the privacy information of the sensor node, then it can masquerade as the sensor to collapse the protocol. In addition, sensor nodes closer to the sink suffer from a more traffic load in contrast to other sensor nodes and their energy is dissipated sooner, leading to a shorter network service period [14].

b. Distributed clone detection protocols: With a distributed clone detection protocol, each sensor node chooses onlookers for clone discovery, making it problematic for malevolent users to overhear the communication between the sink and the sensor nodes. There exist three types of witness selection approaches [15]: i) deterministic selection, ii) random selection, and iii) quasi-random selection which are elaborated as follows:

i. The clone detection protocols applying deterministic witness selection approach, such as the Randomized Efficient and Distributed Protocol (RED) allow all sensors to choose the same group of witnesses. The communication overhead can be reduced and a higher clone detection probability can be yielded by selecting similar deterministic group of witnesses [16]. Nevertheless, malevolent users have potential to contaminate some sensor nodes by overhearing communications between the source node and its witnesses in order to gain mapping functions and active spiteful assaults [17].

ii. To remove the shortcomings, clone detection protocols using random witness selection strategy have been proposed, such as the Line-Select Multicast Protocol (LSM). Each sensor's witnesses are randomly mapped to a node's identity, making it more challenging for malevolent users to get the witnesses' information, even if they overhear the communication between the sensor node and the sink node. At the other side [18], the randomness in the mapping function makes it challenging for the source node to efficaciously notice its witnesses, which reduces the chances of clone finding. Thus, clone detection probability is amongst the fundamental performance measures for security assessment in the clone detection protocols implementing random witness selection strategy.

iii. Clone detection protocols implementing semi-random witness selection strategy like single deterministic cell (SDC) [19] aim to create a balance between the random and deterministic witness selection schemes. In the semi-random scheme, the mapping function produces a deterministic region for every sensor device, and witnesses are chosen from this region on random basis. This scheme needs huge communication overhead and intricacy because the sensors have different sets of witnesses [20]. In addition, because of the restricted power of battery, network service period is a crucial performance parameter in wireless sensor networks [21].

II. LITERATURE REVIEW

2.1 Detection of Replication Attack using Optimization Techniques and Machine Learning

S. Anitha, et.al (2020) suggested an effectual application in which diverse techniques such as EMABRD (Exponential Moving Average based Replica Detection), SACOP (Secured Ant Colony Optimization) and FZKA (Fingerprint based Zero Knowledge Authentication) were presented on the real time environment [22]. The results of comparison revealed the superiority of the SACOP over others for offering higher probability to detect the malicious nodes with regard to maximum storage and communicating overheads. Moreover, the EMABRD performed more effectively with regard to overheads.

L. S. Sindhuja, et.al (2018) discussed that the HCMS (healthcare monitoring system) faced a major issue of security due to the vulnerability of this system towards diverse attacks and the node replication was a main attack that led to impact the reliable and confidential data [23]. An AIS (Artificial Immune System) based technique recognized as EHIP-HOP technique was introduced on HCMS for detecting the node replica attack in an environment having limited resources and at lower cost. The results demonstrated that the introduced technique was resisted against the attacks more robustly with regard to overhead, throughput, PDR (packet delivery ratio) and energy usage.

P. Sherubha, et.al (2019) developed a technique for detecting a number of replica attacks in WSN (Wireless Sensor Network) [24]. Moreover, this technique emphasized on formulating an adaptive RF-MOCS (Random Forest based Multi-Objective Cuckoo Search) algorithm for recognizing the source of clone attack. The developed technique was quantified on KDD cup dataset. The developed technique performed well concerning accuracy, sensitivity, specificity and F-measure. The results exhibited that the developed technique outperformed the traditional methods.

Table 1: Detection of Replication Attack using Optimization Techniques and Machine Learning

Author	Year	Technique Used	Findings	Limitations
S. Anitha, et.al	2020	EMABRD (Exponential Moving Average based Replica Detection), SACOP (Secured Ant Colony Optimization) and FZKA (Fingerprint based Zero Knowledge Authentication)	The results of comparison revealed the superiority of the SACOP for offering higher probability to detect the malicious nodes with regard to maximum storage and communicating overheads. Moreover, the EMABRD performed more effectively with regard to overheads.	The suggested application attained misdetection in case of arrival of events at random.
L. S. Sindhuja, et.al	2018	EHIP- HOP technique	The results demonstrated that the introduced technique was resisted against the attacks more robustly with regard to overhead, throughput, PDR (packet delivery ratio) and energy usage.	The issue related to the failure of single point was often occurred in such technique.

P. Sherubha, et.al	2019	RF-MOCS (Random Forest based Multi-Objective Cuckoo Search) algorithm	The developed technique performed well concerning accuracy, sensitivity, specificity and F-measure. The results exhibited that the developed technique outperformed the traditional methods.	This technique provided poor performance on other datasets while predicting the presence of clone attack in WSN (Wireless Sensor Network).

2.2 Detection of Replication Attack using Key Management Techniques

L. Li, et.al (2020) established a SRKD (secure random key distribution) technique which was focused on generating an innovative technique to defend against the replication attack [25]. In particular, a localized algorithm was integrated with a voting system for detecting and eliminating the malicious nodes. The replica attack was prevented by changing the meaning of metric. The results of experiments depicted that the established technique offered success rate of 90% above for detecting the replicate nodes in the availability of two hundred nodes in network. Moreover, the established technique was proved efficient and secure, and provided more enhanced storage and communicating efficacy as compared to the conventional techniques.

M. Buragohain, et.al (2018) constructed a new key management technique. The fundamental goal of this technique was to diminish the computing overhead, mitigate the communicating overhead, lessen the impact of node capture attack, and protect the node from known attacks such as clone attack and replay attack [26]. The identity-based cryptography was put forward in which the bilinear pairing was employed on ECs (elliptic curves). Strand Space model was exploited to illustrate that the constructed technique was secure. The simulation results indicated that the constructed technique performed well in comparison with other protocol concerning computing time.

M. Perez-Jiménez, et.al (2019) projected a novel technique to allocate the signature in WSN (Wireless Sensor Network) on the basis of magnetic PUF (Physical Unclonable Function) [27]. The Physical Unclonable Function utilized the physical properties for generating the private keys. It was not possible to access these keys and replicate them. This resulted in inserting the intrinsic complexity magnetic phenomena using which an unbreakable signature technique was described. The simulation was conducted for evaluating the projected technique. The results revealed that the projected technique provided higher entropy and had potential for producing a huge catalogue of diverse keys.

Table 2: Detection of Replication Attack using Key Management Techniques

Author	Year	Technique Used	Findings	Limitations
L. Li, et.al	2020	SRKD (secure random key distribution) technique	The results of experiments depicted that the established technique offered success rate of 90% above for detecting the replicate nodes in the availability of two hundred nodes in network. Moreover, the established technique provided more enhanced storage and communicating efficacy.	This technique had not offered surety for the connectivity of network and unable to prevent the attack in complex some scenario.
M. Buragohain, et.al	2018	A new key management technique	The constructed technique was inefficient to enhance the energy utilization and to optimize the energy efficacy.	The simulation results indicated that the constructed technique performed well in comparison with other protocol concerning computing time.
M. Perez-Jiménez, et.al	2019	Magnetic PUF (Physical Unclonable Function) based technique	The results revealed that the projected technique provided higher entropy and it had potential for producing a huge catalogue of diverse keys.	The projected technique was not able to produce complex keys.

2.3 Detection of Replication Attack using Watermarking Techniques

V. -T. Nguyen, et.al (2018) suggested a new watermarking technique with the objective of resisting against fake or clone node ID attacks and protecting the sensed data at the same time [28]. The suggested technique proved more secure and robust, and it was easy to integrate this technique with a practical routing algorithm on the basis of dynamic watermark. The suggested technique offered higher energy efficacy when this technique was integrated with LEACH (Low Energy Adaptive Clustering Hierarchy) protocol. The results obtained in analyzing the security validated that the suggested technique was efficient.

T. Hoang, et.al (2020) described that the node replication attacks led to generate a conflict of inside intrusions due to which the efficacy of the sensor networks was damaged at large extent [29]. Thus, a new lightweight mixed secure technique was investigated on the basis of watermarking method with the purpose of protecting sensory data and resisting against node clone attacks. The investigated technique was evaluated by conducting numerical and security analysis. The simulation results confirmed that the investigated technique provided consistency and resistance.

Mojtaba Jamshidi, et.al (2020) presented a three-stage methodology for detecting the replica nodes [30]. The watchdog nodes were considered in this methodology which was planned on the basis of concept that the similar opportunity was given to all nodes for meeting with the watchdog nodes. The network traffic was monitored and the channel was observed using the watchdog nodes. The J-SIM simulator was applied to conduct a series of simulations so that the efficacy of the presented methodology was computed with respect to the probability to detect the replication node and false detection probability. The simulation results depicted that the presented methodology was applicable for detecting the replicated nodes and mitigating the false detection probability 0.005% below.

Table 3: Detection of Replication Attack using Watermarking Techniques

Author	Year	Technique Used	Findings	Limitations
V. -T. Nguyen, et.al	2018	A new watermarking technique	The results obtained in analyzing the security validated that the suggested technique was efficient.	The suggested technique was not changed the duration of the WSN (wireless sensor network) as much after its integration with the watermark procedure.
T. Hoang, et.al	2020	A new lightweight mixed secure technique	The simulation results confirmed that the investigated technique provided consistency and resistance.	The response of WSN (Wireless Sensor Network) was the major limitation of this technique in an attack was detected.
Mojtaba Jamshidi, et.al	2020	A three-stage methodology	The simulation results depicted that the presented methodology was applicable for detecting the replicated nodes and mitigating the false detection probability 0.005% below.	The presented methodology had a slight delay to recognize the replicated nodes due to which the malicious nodes attained an opportunity for performing the operations in the network.

III. RESEARCH METHODOLOGY

Following are the various phases of detection of malicious nodes:-

1. Pre-Processing:- The wireless sensor network is configured with fixed amount of sensor nodes. The clustering on the basis of locality is applied in the entire network. In the proposed LEACH protocol, power and remoteness of each node is verified correctly. The node having utmost power and least distance is selected as the cluster head. The whole nodes occurring in the network will send their information to the cluster head. The cluster head further creates path with the help of other cluster heads and propels this information to the base station. AODV routing protocol is utilized for the establishment of path among source and the destination. AODV protocol is a source node protocol which deluges the route reply packets. The source node selects the most appropriate route towards the destination according to the hop count and highest sequence number.

2. Detection of malicious nodes: - A number of approaches were proposed in the last few years for the discovery of attacker nodes. The earlier method was monitor mode method. The activity of the neighboring node can be observed with the help of this method. This method does not give good performance in the recognition of attacker node. The second method implemented in the earlier investigation was named as delay tolerance method. This method needs extra hardware and software for the discovery of attacker nodes. This increases the intricacy and cost of the arrangement. The base station applies node localization method for the discovery and segregation of attacker nodes. The node localization technique gathers data on the basis of established route. The base station can collect the whole data of sensor nodes with the help of node localization method. The base station can collect data about the location of sensor node and their delay during the information transmission. The base station scrutinizes the quality of service constraints. When the network throughput is decreased to threshold value, then base station takes action for the discovery of attacker node. The base station checks the network throughput on every hop for the detection of attacker node form the network. The node which decreased the throughput below the threshold value is identified as the attacker node. The gathered data comprises the remoteness of each node from the base station. The distance creates delay in every hop count which exists on the formed route. The base station detects this delay. The delay of every hop is calculated due to which node will enhance the delay within the network and identifies the attacker nodes.

IV. CONCLUSION

Wireless Sensor Network can be described as a self-organized and infrastructure less wireless network of sensor nodes. These sensor nodes perform the monitoring of physical or environmental conditions such as humidity, sound, vibration etc. The sensor nodes collectively forward their data via the network to a base station or sink. At base station, the observing and analysis of data can be done. A sink or base station acts as a link between users and the network. It is possible to extract necessary information from the network by inserting queries and collecting outcomes from the base station. The various schemes are analysed which increase security of the network. In future, novel scheme will be designed to increase security of wireless sensor networks.

V. REFERENCES

[1] M. N. I. Khan and M. S. Islam, "A New Scheme to Detect and Prevent Node Replication Attacks for Wireless Sensor Networks," 2019 International Conference on Computer Communication and Informatics (ICCCI), 2019, pp. 1-5

[2] B. Shimpi and S. Shrivastava, "A modified algorithm and protocol for Replication attack and prevention for Wireless sensor Networks," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016, pp. 1-5

[3] Y. -S. Ho, R. -L. Ma, C. -E. Sung, I. -C. Tsai, L. -W. Kang and C. -M. Yu, "Deterministic detection of node replication attacks in sensor networks," 2015 IEEE International Conference on Consumer Electronics - Taiwan, 2015, pp. 468-469,

[4] H. Kaur and S. Saxena, "A review on node replication attack identification schemes in WSN," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1-8

[5] M. Qabulio, Y. A. Malkani and A. Keerio, "Securing mobile Wireless Sensor Networks (WSNs) against Clone Node Attack," 2015 Conference on Information Assurance and Cyber Security (CIACS), 2015, pp. 50-55

[6] M. Numan et al., "A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 65450-65461, 2020

[7] C. -M. Yu, C. -S. Lu and S. -Y. Kuo, "Compressed Sensing-Based Clone Identification in Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 3071-3084, April 2016

[8] T. P. Rani and C. Jayakumar, “Unique identity and localization based replica node detection in hierarchical wireless sensor networks”, Computers & Electrical Engineering, vol. 7, no. 4, pp. 239-244, Nov. 2017

[9] P. Abinaya and C. Geetha, "Dynamic detection of node replication attacks using X-RED in wireless sensor networks," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-4

[10] S. Roy and M. J. Nene, "Prevention of node replication in Wireless Sensor Network using Received Signal Strength Indicator, Link Quality Indicator and Packet Sequence Number," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 2016, pp. 1-8

[11] W. Z. Khan, M. S. Hossain and M. Atiquzzaman, “A cost analysis framework for claimer reporter witness based clone detection schemes in WSNs”, Journal of Network and Computer Applications, vol. 2, no. 9, pp. 261-267, March 2016

[12] P. P. Devi and B. Jaison, “Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms”, Computer Communications, vol. 1, no. 18, pp. 967-975, 1 Feb. 2020

[13] U. Iqbal and A. H. Mir, “Secure and practical access control mechanism for WSN with node privacy”, Journal of King Saud University - Computer and Information Sciences, vol. 15, no. 7, pp. 1013-1021, 26 May 2020

[14] K. Farah and L. Nabila, "The MCD Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," 2014 International Conference on

Advanced Networking Distributed Systems and Applications, 2014, pp. 58-63

[15] L. Yang, C. Ding and M. Wu, "Location Similarity Based Replica Node Detection for Sensor Networks," 2016 9th International Symposium on Computational Intelligence and Design (ISCID), 2016, pp. 56-59

[16] L. Sujihelen and C. Senthilsingh, "Detect the replica node in Mobile Wireless Sensor Networks," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 265-267

[17] L. Sujihelen, M. Satyanarayana and C. Senthilsingh, "Replica Node Detection in Distributed Wireless Sensor Networks," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 704-707

[18] W. Z. Khan, M. Y. Aalsalem, N. M. Saad, Y. Xaing and T. H. Luan, "Detecting replicated nodes in Wireless Sensor Networks using random walks and network division," 2014 IEEE Wireless Communications and Networking Conference (WCNC), 2014, pp. 2623-2628

[19] G. Cheng, S. Guo, Y. Yang and F. Wang, "Replication attack detection with monitor nodes in clustered wireless sensor networks," 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), 2015, pp. 1-8

[20] M. M. Singh, A. Singh and J. K. Mandal, "Preventing node replication attack in static Wireless Sensor Netwroks," Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, 2014, pp. 1-5

[21] A. Rani and S. Kumar, "A low complexity security algorithm for wireless sensor networks," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1-5

[22] S. Anitha, P. Jayanthi, and V. Chandrasekaran, “An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks”, Measurement, vol. 5, no. 12, pp. 8022-8030, 2020

[23] L. S. Sindhuja, "Security of Healthcare Monitoring System using EHIP-HOP method," 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), 2018, pp. 199-204

[24] P. Sherubha, P. Amudhavalli and S. P. Sasirekha, "Clone Attack Detection using Random Forest and Multi Objective Cuckoo Search Classification," 2019 International Conference on Communication and Signal Processing (ICCSP), 2019, pp. 0450-0454

[25] L. Li et al., "A Secure Random Key Distribution Scheme Against Node Replication Attacks in Industrial Wireless Sensor Systems," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2091-2101, March 2020

[26] M. Buragohain and N. Sarma, "PKSN: A pairing based key management scheme for heterogeneous sensor network," 2018 10th International Conference on Communication Systems & Networks (COMSNETS), 2018, pp. 198-205

[27] M. Perez-Jiménez, B. Bordel, A. Migliorini and R. Alcarria, "An Automatic Key Generator based on Physical Functions for Resource Constrained Nodes in Future Wireless Sensor Networks," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-6

[28] V. -T. Nguyen, V. -H. Bui, T. -T. Nguyen and T. -M. Hoang, "A Novel Watermarking Scheme to against Fake Node Identification Attacks in WSNs," 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), 2018, pp. 1-5

[29] T. Hoang, V. Bui, N. Vu and D. Hoang, "A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks," 2020 International Conference on Information Networking (ICOIN), 2020, pp. 649-653

[30] M. Jamshidi, S. S. A. Poor and M. R. Meybodi, “A simple, lightweight, and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information”, Ad Hoc Networks, vol. 4, no. 23, pp. 415-427, 29 Jan. 2020