International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Survey of Recent Research Methodologies for the Security Provisioning in Wireless Sensor Networks

Vanita Verma*,[1], Dr. Vijay Kumar Jha[2]

Submitted: 28/01/2024 **Revised**: 06/03/2024 **Accepted**: 14/03/2024

Abstract: Introduction**:** Wireless Sensor Network (WSN) is evolved as one amidst the supremely valuable technologies aimed at the forthcoming future.

Objectives: Nodes prevalent inside a WSN are exposed to diverse attacks largely as a reason of their nature of utilizations, like restricted storage and as well less-power of sensor nodes (SNs).

Methods: Therefore, providing security aimed at the network becomes a big challenge. The active research areas aimed at WSN security comes with several topics, namely secure routing, secured authentication, key management (KM), intrusion detection (ID) frameworks, trust mechanisms, and secured data aggregation (cluster-centred routing). Diverse methodologies are established in the topics above aimed at providing WSN security. However, it is tough to choose which scheme is best in an explicit WSN application.

Results: So, this work proffers an assessment of current research methods developed for WSN security in the above-mentioned schemes. The latest research topics' review for WSN's security is presented with the methodologies utilized, advantages, and limitations that can facilitate the researchers to acquire the finest security solutions aimed at the particular application of WSN.

Conclusion: Finally, the study identifies diverse open research difficulties that should be examined in the forthcoming future.

Key words: *Wireless Sensor Network (WSN), WSN security, Authentication, Trust based WSN security, Cryptographic algorithms, Key management, secure routing.*

1. Introduction

WSNs (Vinita Daiya et al. 2019; Alexey G Finogeev and Anton A. Finogeev, 2017) comprises numerous SNs (GhasemFarjamni et al. 2019) scattered. A distributed group of sensors prevalent in these networks creates a network interconnected via the wireless communication links, and every sensor function as an information source sensing and also gathering data as of its environment and transmitted them onto a base station (BS) (SatheesBabu S and BalasubadraK, 2019) or sink in a multi-hop fashion (Abdul HamidMd and JehadSarkarAM, 2012). The WSN's features are restricted power supply, less bandwidth, lesser memory sizes, and also restricted energy consumption (EC) (Ilango P, 2015). The WSN comprising heterogeneity has an extensive view in life and is extensively utilized in numerous fields, namely industrial work monitoring and also control, wildlife monitoring, medical applications, home automation, defense applications, etcetera (Fan Wu et al. 2017). WSN suffers as of challenges, namely energy and data security management. They include attacks as of intruders that are a portion of the network and also outside (Ashok Kumar Das, 2016). There exist diverse possible attack kinds on WSN, namely routing attacks, Sybil attacks, and also denial of service (DoS), etcetera. Fig-1 exhibits the diverse likelihoods of attacks prevalent in WSN. A malevolent node declines randomly aimed at dropping the packets or else forwarding the communications. There exists no necessity aimed at fixing those nodes' positions since the SNs are applicable for the high-risk field.

*[*1] Research Scholar, Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi-835215(JH), India*

*[*1] Email ID: vanithaphd123@yahoo.com*

[2] Associate professor, Department of Computer Science and Engineering, Birla Institute of Technology, MesraRanchi-835215(JH), India

[2] Email ID: vkjha@bitmesra.ac.in

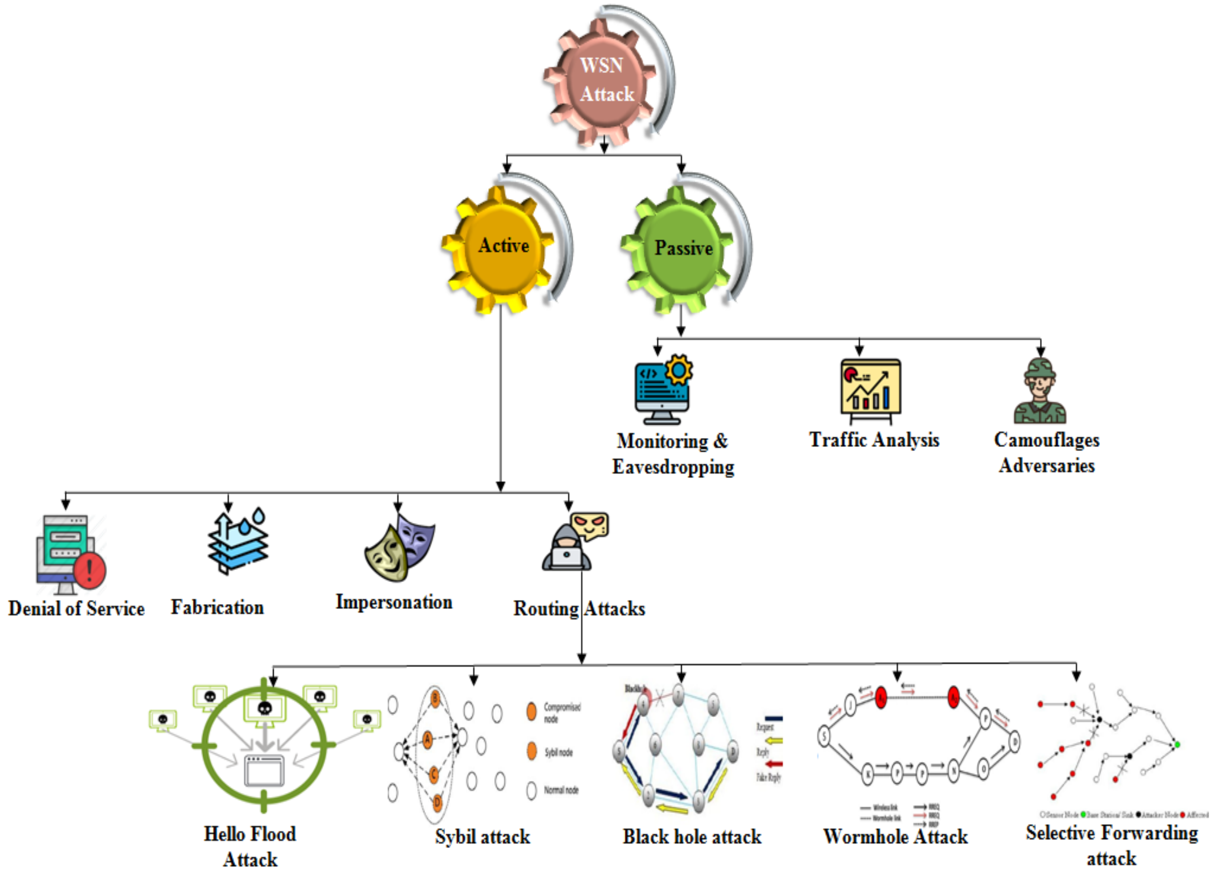


Fig 1: Attacks in WSN

Hence, there exists no security aimed at majority of the WSNs that evades the simple intrusions on the SNs (Deepak C Mehetre et al. 2019). This directs towards a situation of attacks that causes false traffic inside the network (Suryaprabha E and SaravanaKumarNM, 2019). Henceforth, security has become one amidst the prime concerns whilst there exist potential attacks towards sensor networks. Security permits WSN to be utilized with guarantee. With no security, the WSN's utilization in whichever application region would yield unwanted consequences (Sunil Gupta et al. 2014). A few studies recommend that the encryption methodologies can repel attacks as of outside however usually is powerless whilst attacks are thrown by nodes inside the network (Xiang Gu et al. 2017). ID systems (IDSs) are employed in WSN aimed at detecting the nodes' malevolent behavior inside the WSN. IDS-centred systems are much efficient aimed at finding the irregular actions of the networks' inner nodes, averting the total network as of diverse malevolent attack types (Gautam M Borkar et al. 2019). Likewise, trust-centred approaches are available that can find the malevolent behaviors prevalent inside the network in lieu of the conventional security techniques. Moreover, the protocols centred upon the information security principles, namely integrity, confidentiality, non-repudiation, authentication, and also obtainability, have been built for the security weaknesses (AykutKarakaya, and SedatAkleylek, 2018). Fig-2 exhibits WSN's security solutions.

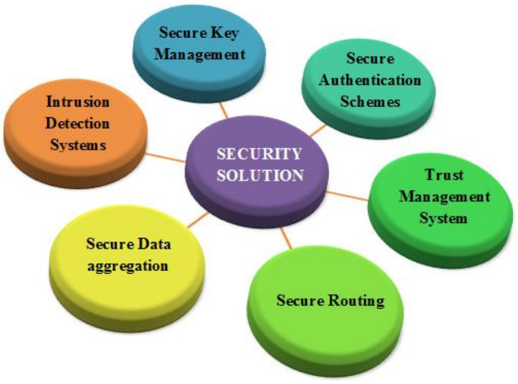


Fig 2: Security solutions to WSN

Until now, a surfeit of security resolutions and also authentication techniques are recommended by researchers over the past '2' years (BhawnaNarwal, and Amar Kumar Mohapatra, 2020). It is tough to choose which scheme prevalent in a certain WSN application apt best. This work proffers an assessment on what way the assets of diverse trust management (TM), authentication, routing, KM, and also intrusion methodologies are employed aimed at particular WSN applications. Centred on this review, the techniques, advantages, and restrictions of the previously proposed authentication, KM, TM, routing mechanism, and also intrusion-centred security techniques are proffered, also pointed future research directions to look for the novel security solutions.

2. Literature Review

Herein, the security-centred on authentication techniques, KM, TM, routing schemes, and also intrusion methodologies are systematically examined and reviewed. This work briefly explicates the research development on WSN network security centred on the above '5' aspects via summarizing and also observing these outcomes, their pros as well as cons, and as well pointed restriction future research's direction aimed at searching the advanced security solutions. This paper's remaining part is systematized as: section 2.1 explicates diverse security solutions centred on authentication methodologies; section 2.2 reviewed the KM techniques aimed at WSN security; section 2.3 surveyed the diverse trust models; section 2.4 studies the diverse secure routing methodologies prevalent in WSN; section 2.5 elucidates the diverse ID centred secured techniques aimed at WSN; section 2.6 presented the results' analogy of the diverse studied techniques aimed at WSN security; section 3 concludes a few challenges and also opportunities prevalent within this field, and detects the possible future directions.

2.1 Authentication Schemes

During past years, diverse authentication methodologies are recommended aimed at overcoming the security feebleness of the data's capturing and accessing procedure by the WSN. The authentication technique functions as a needed part aimed at inquiring and spreading the WSNs' real-time data securely via diverse cryptography methodologies, namely RSA, hashing protocols, and also ECC. This section offers the diverse authentication schemes' reviews that are recently proffered aimed at defeating the WSN's common attacks.

Rosheen Qazi *et al.* (2020) presented a security protocol utilizing the ECC algorithm aimed at offering authentication on every single node such that just the authenticated nodes could converse with one another. The model offered security aimed at the node-to-node communication network and also hoarded memory space prevalent on nodes utilizing Elliptic Curve Digital Signature (ECDSA) technique. The Algorithm aimed at Wireless Secure Communication (ASCW) provided KM utilizing acceptable key length. Also, it decremented the security intimidations and cost of risk on the network utilizing an authentication methodology. Results signified that ASCW was one amidst the apt approaches aimed at securing the data on nodes during the communication in WSN. However, the network's deployment time could significantly distress the keys' formation on the nodes.

Vaniprabha. A and Poongodi. P (2019) presented an augmented lightweight security protocol utilizing an access control design aimed at wireless medical sensor networks. First, an attack model was constructed aimed at the wormhole, Sybil, and also sinkhole attacks and identified those attacks underneath diverse constraints. Second, an effective weighted product design was developed that transmitted the patients' sensed data centred upon their emergency. Then, enhanced ECC permitted data access aimed at the authorized users. The attack model attained 97% PDR and the security design spent 2.4s and also 0.96s time aimed at secret key's generation time and secret key's exchange procedure. However, in a few circumstances, as a reason of the location's restriction, the patient's data can't be accessed by the technicians.

Chandra Sekhar *et al.* (2017) designed a smart card-centred authentication protocol aimed at ensuring secured and authorized communication inside the WSN. The scheme comprised diverse security features and also friendliness nurturing usable features. The security assessment of every key's security feature in the designed techniques had been analyzed. The design was simulated aimed at the proper security verification utilizing the extensively-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The results exhibited that the technique was safeguarded from the passive and also active attacks comprising the replay and also man-in-the-middle attacks. Nevertheless, the technique was exposed to diverse practical attacks, which might direct towards unplanned consequences.

Huei-Wen Fern and Nguyen Minh Khoa (2017) presented a security protocol termed DSEDA aimed at ensuring end-to-end data authentication (DA) in cluster-centred WSN. DSEDA employed CH aimed at verifying the report at the reported lifetime's very beginning so the bogus report could be plunged as early as possible. Centred on the digital signature, an en-route filtering technique was executed utilizing DSEDA aimed at evading intermediate nodes as of forgery or else untruthful information. As of the examination outcomes, it was validated that the DSEDA considerably outshined LEDS regarding the security strength and also the performance. But DSEDA's performance was little poor under the selective forwarding attack.

Dheerendra Mishra *et al.* (2019) presented a robust authentication technique utilizing a smartcard aimed at resolving the security complications in IoT-enabled WSN. The proof of mutual authentication's perfection was executed utilizing the BAN logic design. Moreover, the additional security examination claimed tough protection against the well-known security attacks. The protocol was assessed widely and analogized against identical methodologies and the outcomes exhibit that it is proficient and tough analogized to the earlier protocols. However, the protocol's complexity was slightly greater analogized to the existent techniques.

Qi Jiang *et al.* (2019) presented an improved '2'-factor authentication technique with unlink-ability aimed at WSN. The scheme cut the computation's cost. Hence, the technique not just solves its security errors nevertheless also boosted its performance. The scheme provided relatively added security attributes, namely flexibility of feeble stolen smart card attacks, user's anonymity, and unlink-ability, with not producing excessive overhead. The model was prone to several routing attacks.

Mostafa H. Dahshan (2019) presented a robust DA technique aimed at shielding the data's integrity and as well its availability inside the unattended WSN. The technique presented combined security against data's modification and DoS attacks comprising traffic and also storage efficacy. A detailed comparative analysis was performed with '4' related technique and exhibited that the technique performed close or better analogized to all these protocols on the '4' mentioned metrics.

Lina Yang *et al.* (2019) presented a Hierarchical Hash Tree technique with less overhead aimed at boosting the protocols' security. The scheme comprised '2' layers of Merkle Tree centred on the concepts of hierarchy and also aggregation. The scheme was utilized aimed at implementing the Sreluge protocol's page authentication that was a representative reprogramming procedure centred upon arbitrary linear codes. The scheme cut the authentication overhead by 43 % Merkle Tree and also other overheads were decremented prominently with the code image's growing size. TheMerkle trees' drawback (against other tree types) included higher CPU usage and memory footprints. Table-1 explicates the diverse authentication scheme's types aimed at WSN's security with their benefits and also their disadvantages.

Table 1: Various authentication mechanisms for WSNs security

Author	**Technique used**	**Tool used**	**Advantages**	**Disadvantages**
Haitao Yu and Liejun Wang (2019)	Security-improved mutual authentication technique centred on the smart card	BAN logic analysis tool	Secured against almost known attacks	Consumed slightly more computational time analogized to other techniques.
Fan Wu *et al.* (2017)	Two-factor authentication technique aimed at WSN centred on ECC	Proverif protocol analysis tool for formal verification	Prevented the network as of an insider attack, user forgery attack, offline guessing attack, etc.	When worked with resource-constrained IoT sensors, ECC scalar multiplication spends the greatest extent of time.
Hong Yu *et al.* (2013)	End-to-end secure communication (utilizing asymmetric authentication and KM) technique for Wisdom Web of Things (W2T) in WSN	Not used any tool. Here, qualitative analysis is performed regarding computation, communication storage and latency.	i) Protected the user's privacy and also key negotiation materials. ii) Blocked DoS attacks at WSN's entrance.	The experiments weren't executed aimed at validating the outcomes in real applications.
Bo Sung Kim and JooSeok Song (2019)	Energy-effective and also secured mobile node reauthentication (ESMR) technique	AVISPA tool	ESMR met MWSN's security necessities and can avert the related security attacks.	ESMR was just employed in a single-hop communication environment and had considerably

	aimed at Mobile WSN			incremented the total EC.
Jangirala Srinivas *et al.* (2018)	Biometric-centred authentication and also key agreement methodology	BAN logic	Satisfies desirable security attacks aimed at the authentication methodology.	The methodology doesn’t facilitate the biometric update process.
Jangirala Srinivas *et al.* (2017)	Symmetric key-centred authentication procedure aimed at WMSN	AVISPA tool	Reached the high-level of security necessities and as well had appropriate performance cost.	Failed to preserve user’s anonymity, man-in-the-middle attack, forgery attack, and also impersonation attack.
Amir Hosein et al. (2019)	Lightweight and also anonymous ‘3’-factor authentication and also access control technique	BAN-logic	Suited for resource-constrained SNs. Attained lowest EC of the SN, communication cost, and also running time.	The lightweight techniques generally have significant security weaknesses.
Jian-Jun Yuan (2014)	Progressed two-factor user authentication in WSN	GNY logic	Provides non-repudiation, protection against the attack as a reason of the lost smart card, and ensured mutual authentication betwixt the GW-node and the user	The scheme was susceptible to information leakage attacks and lacked forward security.

2.2 Key Management Schemes

Aimed at authenticating a node's identity or else its information, concerning cryptography, a key function as an extremely vital part. An apt-key generation methodology is necessary for the WSN’s security. Key generation protocols are symmetric or else asymmetric natured. The key generation’s symmetric mode is appropriate for the SNs’ efficient working since they spend lesser time and power (Alma E Guerrero-Sanchez et al. 2020). This section surveys diverse KM techniques recently for providing WSN security.

T. Lalitha and S. Jayaprabha (2016) presented a mobility management methodology for WSN’s keying technique. Firstly, the clusters were formed and the CH was selected centred on some requirements. Then, the cluster keys and also pair-wise keys were produced by the sink via exclusion basis systems. The mobility-centred KM methodology was triggered each time a node shifts as of a presently connected cluster to the other prevalent inside the network. A key organization protocol ensured the nodes’ forward and backward secrecy. The technique attained the finest results regarding EC. Here, the data’s collection was performed by CH. This might yield unwanted data that wastes the sensor’s power.

S. Soderi (2020) described the employment of the watermark-centred blind physical layer security (WBPLSec) towards acoustic communications as a progressive wireless link. It combined watermarking and also jamming methodologies over sound-waves aimed at creating a secured area nearby the legitimate receiver. The scheme addressed counter-measures against confidentiality attacks on short-range wireless communications. The outcomes explicated that this methodology was a treasured technique aimed at employing physical layer security by generating a secured area around the receiver up to 2m. The prime problem was—if the respective chip flip positions were erroneous, then the watermark signal won't be discovered and the frame might be dropped.

Khaled Hamouid *et al.* (2020) presented a light-weight and secured tree-centred routing technique (LSTR) aimed at WSN. The data routing's security as of SNs to the BS was achieved centred on an effective ID-centred authenticated key-agreement methodology. The procedure significantly decremented the communication overheads by 70–90% in analogy to PMMTK, DKMM, and also SEHKM techniques. Additionally, the storage requirements and EC were considerably reduced. But, the methodology comprises diverse demerits, like replay attack, user's anonymity, no effective password/biometric update procedure.

Yanrong Lu *et al.* (2019) proffered an anonymous '3'-factor key agreement utilizing ECC for WSN. The mutual authentication properties were ensured by employing the Burrows–Abadi–Needham logic. The security examination exhibited that the protocol resists the diverse attacks. However, the design suffered from recognized session-specific temporary information attacks that directed towards the session keys' disclosure in other sessions. Moreover, the model was weak to track attacks and also fails aimed at satisfying the user's intractability.

Mohammad Sadegh Yousefpoor and Hamid Barati (2020) presented a smart dynamic KM system for WSN that utilized fuzzy logic aimed at path key generation and aimed at involving new nodes into the network. The fuzzy logic's utilization in the KM system resulted in incremented accuracy in decision making and also contributed towards its smartification. Analogized to other KM systems, the scheme presented was much effective regarding communication overload, requisite memory space, and also EC. The system elucidated suitable resilience and also resistance towards cryptanalysis attacks. But setting exact fuzzy rules and membership functions is a tough task.

2.3 Trust Models for Network Security

This section reviews diverse trust-centred secure protocols aimed at WSN's support. A few methodologies identified are examined here.

Tianshu Wang *et al.* (2019) presented a trust enhancement protocol aimed at cluster-centred WSN, where network time was split to numerous rounds. Every round comprised a setup stage and a steady-state stage. In the setup stage, clusters were created and also the mutual trusted relationships betwixt the cluster nodes were built via Setup μTESLA and SET-SCHNORR. In the steady-state segment, physical data collected were conveyed via the STEADY-μTESLA methodology. The protocol performs effectively in repelling attacks like these as data integrity attacks, data confidentiality attacks, and also negotiation the node attacks. But, the TPM wasn't applied on a real SN of the real WSN in the industry.

Tong Zhang *et al.* (2018) presented a trust evaluation methodology aimed at the clustered WSN centred on a cloud design that implemented the conversion betwixt qualitative and quantitative of SNs' trust metrics aimed at attaining efficient trust evaluation. The methodology could identify polytype malevolent attacks that include bad-mouth attack, black hole attack, selfish behavior attack, on-off attack, Sybil attack analyzed as of attack types, and also involves faked ID attack, communication link attack, data attack and also energy attack analyzed as of attack targets. But the model did not perform any routing mechanism that makes the network liable to routing attack varieties.

Xueqiang Yin and Shining Li (2019) presented a trust evaluation design utilizing entropy-centred weight assignment aimed at malevolent node's detection within WSNs. Aimed at boosting the trust quantification's validity and ensuring the evaluation's objectivity, the entropy weight methodology was implemented aimed at determining the proper weight's value. Analogized with the prevalent methodologies, the design could decrement the malicious nodes' impact much efficiently. However, the methodology didn't perform any clustering procedure for proficient data transmission that led to high EC, high bandwidth demand, and also quality of service (QoS) provisioning.

S. Ramesh and C. Yaashuwanth (2020) presented a light-weight trust decision-making methodology aimed at QoS clustering for offering secured routing within inter-cluster and also intra-cluster communication. The LEACH protocol was adapted aimed at the group formation and as well aimed at the trust values' exchange amidst the member nodes, master nodes, and also BS. This system was as well lightweighted as it required just the simple arithmetic computation and consumed fewer number resources. The negatives of utilizing LEACH was that aimed at any reason CH dies, the cluster will become unusable since the data gathered via the cluster nodes would never attain its destination (i.e.) BS.

Osama Al Farraj *et al.*(2018) presented an activation function-centred trusted neighbor selection (AF-TNS) aimed at resource-constrained WSN aimed at boosting the network's security. AF-TNS technique guaranteed minimal delay (8.5 s), higher throughput (149 kbs), minimal energy (8.53 J), and also greater network's lifetime (390 s), and as well comprised lesser false detective rate (1.5%) whilst communicating the network's information. Although, the AF-TNS methodology offered trust in the wireless network, the network comprised limitations whilst administering the trust and also related routing points.

Table 2: Survey of different trust-based models

Author	Description and Drawbacks
M. S. Sumalath and V. Nandalal (2020)	Presented a cross-layer security-centred fuzzy trust calculation mechanism (CLS-FTCM) aimed at detecting malevolent nodes in WSN. But the model doesn't safeguard the network as of the attacks, namely impersonation attack, Sybil attack, wormhole attack, and also man-in-the-middle attack.
A. Ranjith Kumar and A. Sivagami (2020)	Proffered a Fuzzy-logic system aimed at malevolent node's detection, which calculated the trust score aimed at each SN prevalent inside the network. For data security, Improved Elliptic Curve Cryptography (IECC) was presented. But the computation complication had been increased as a reason of the hybrid techniques' presentation.
V. R. SarmaDhulipala*et al.* (2013)	Presented a heuristic technique-centred trustworthy architecture aimed at WSN. The work wasn't tested with more attributes, like accuracy, scalability, and fault tolerance.
P. N. Renjith (2020)	Presented a Trust-centred Routing solution with the employment of ANFIS and NN utilizing the Trust algorithm. But, ANFIS suffers as of the restrictions that halt applications in difficulties with large inputs, like, the curse of dimensionality and also computational expense.

2.4 Routing Schemes

Diverse routing procedures are proffered aimed at secured routing centred upon trust evaluation, EC, and also security. These '3' elements are much essential for reliable communication betwixt nodes prevalent inside the network. This section examines diverse secured routing methodologies that were put forward earlier aimed at WSN's support.

S. Vidhya and T. Sasilatha (2018) presented a multi-layer security protocol (MLSP) utilizing energy power consumption ad-hoc on-demand distance vector (EPC AODV) routing methodology aimed at the secured data transfer in WSN. The shortest route attained in EPC AODV offered reliability. The advanced encryption standard (AES) algorithm was applied on the EPC AODV to code and decode the data. The layer-by-layer interpretation was executed by the MLSP. The MLSP attained a 95% PDR, 90% throughput, and also 0.29 ms end-to-end delay within the network. Nevertheless, the coding and decoding of data using AES in the counter mode were complex to deploy in the software by pondering both performance and security.

M. Yuvaraju and K. A. Pranesh (2020) presented an energy proficient hybrid secure scheme (EPHSS) aimed at providing secured and also energy-proficient data transmissions within WSN. The system utilized two-tier hybrid security designs (ECC and AES) that generated graded co-prime keys aimed at public and also private keys as well as aimed at the node verification procedure. Clustering was performed that decremented redundant energy wasting in node communication. The scheme's efficacy was enumerated by implementing delivery rates of packets that yielded 18% efficiency analogized to the existent scheme. However, the utilization of a hybrid security system (ECC and AES) attained quite intricate computation cost that caused this system's restriction.

Jie Cui *et al* .(2018) presented a secure energy-saving data aggregation technique built aimed at large-scale WSN. The Okamoto-Uchiyama homomorphic encryption technique was utilized aimed at end-to-end data's confidentiality, and the homomorphic MAC methodology was employed to attain end-to-end data integrity. The scheme attained efficient performance in decrementing EC and also particularly decryption delay on the BS was very short. But the model's significant demerit was that homomorphic encryption required either application modifications or dedicated and specialized client-server applications for getting it to work functionally.

Hiren Kumar Deva Sarma *et al*.(2016) developed a Secure Hierarchical and Role-centred Routing Protocol (SHaRP) aimed at Mobile WSN. In SHaRP, the sensor field was split to a few logical clusters and every cluster comprised nodes with diverse roles. Diverse keys were utilized by the nodes comprising diverse roles aimed at message encryption as well as message decryption. The SHaRP attained the finest results regarding throughput, EC, security overhead, and lifetime whilst analogized with DEESR. Nevertheless, nodes died early if nodes move at a greater speed. Greater speed led to frequent topology variations that consecutively instigated more re-transmissions of diverse packet types. As a reason of re-transmissions, added energy is utilized and the nodes' early deaths happen.

R. S. Raghav *et al.*(2020) presented a bio-inspired-centred secure routing methodology with the bee algorithms' aid inside the WSN. The routing protocol included primary scout bee and secondary scout bee aimed at executing routing and also security technique. '3' routing attack kinds were utilized to inspect the protocol, namely food attacks, spoof attacks, and also Sybil attacks. The scheme produced an efficient result, wherein it attained the lowest values for an end-to-end delay and also the packet loss. It improved the network's lifetime with a greater packet delivery ratio (PDR) and as well the scheme's path efficacy was high. The primary and also secondary scout bees' usage forwarded the data with no attackers' interference. However, bee algorithms were suffered from improper exploitation in solving complicated problems.

Michele Tortelli *et al.* (2018) addressed the security, congestion control, and also privacy requirements prevalent within WSN dealing with multimedia data (i.e., images). The S^2 DCC was implemented aimed at making the network tough against the malevolent nodes' presence, and to assure the sensed data's secrecy, or else any other sensitive information communicated onto the sink. However, the method failed to detect the malevolent nodes when an error notification message was received.

Jayanthi Ramasamy and John Singh Kumaresan (2020) presented image encryption and cluster-centred protocol aimed at secured image transmission in WSNs. Elliptic Curve-centred key selection and Hill Cipher-centred encryption methodology were presented, wherein the keys were permuted aimed at incrementing the key's size for suiting the image matrix's size directing to a secured transmission by the images' proficient encryption that was conveyed via WSN. Lastly, a secured transmission protocol utilizing clusters was presented aimed at building the secure routing methodology termed Elliptic curve Hill cipher and Cluster-centred Encrypted Routing procedure to be much efficient with a corresponding increment in the security's decrementation in delay and increment in PDR. However, hill cipher's prime drawback was that it encrypted the identical plaintext blocks to identical ciphertext blocks and can't encrypt images that comprise big single-colour regions.

P. Brindha *et al.*(2019) concentrated on the conception of implementing the encryption techniques on multi-hop routing procedures in WSN. Aimed at attaining a higher security level, '2' encryption methodologies, like lightweight encryption algorithm (LEA), and then two-phase hybrid cryptography algorithm (THCA), were utilized centred upon the data's reliability. The LEA is utilized aimed at transmitting proactive data and the significant reactive data is encrypted via THCA. Aimed at the routing objectives, Augmented Tree-centred Routing (ATR) is employed. The methodology exhibited improved performance regarding control overhead, throughput, and also network's lifetime although there existed a few misbehaving nodes prevalent inside the network. However, the network was vulnerable to the side-channel analysis attack due to LEA ciphers' consumed electric power.

2.5 Intrusion Detection Frameworks

Aimed at protecting WSNs' security, IDS are extensively employed in a wireless environment like this. Herein, an in-depth review of a few recent IDS in WSN is offered.

Ashfaq Hussain Farooqi *et al.*(2013) presented an ID framework for securing WSN as of routing attacks. The system worked in a distributed environment aimed at detecting intrusions by cooperating with the adjacent nodes. It worked in '2' modes: online prevention allowed protection as of those unusual nodes that already were affirmed as malevolent whilst offline detection discovers those nodes that were being negotiated via an adversary in the subsequent time-period. The results exhibited that the specification-centred detection methodology attained a higher detection rate and acquired a low false-positive rate. However, the methodology wasn't tested on the clustering-centred hierarchical routing protocol.

Xin Xiao and Ruirui Zhang (2017) improved the dendritic cell algorithm termed DCA-RT that applied the distributed deployment and executed the real-time ID in WSN. The design abstracted the dendritic cell information fusion procedure, defined the external signals' meanings and its functions, which were applied to WSNS, and determined the dendritic cells' mathematical evolution design. The design achieved good detection performance and attained advantages regarding the system's EC. But the design was centred upon the simulation; there existed no verification on the theoretical results in real WSN.

T. K. Thivakaran and T. Sakthivel (2020)presented GUARD, an ID protocol that proficiently identifying the active routing attacks with a significant decrementation in EC. The GUARD utilized non-cooperative game model and exploited the Fuzzy q-learning's advantage aimed at determining the malevolent activity. The methodology decremented the NN's overhead, and thus, makes the system lightweight and to function easily. However, the only consideration is the node's mobility and density. However, this consideration will not change the NN structure other than the inputted parameters.

C. Umarani and S. Kannan (2020) presented a Hybrid Anomaly Detection Systems (HADS) termed Artificial Immune System in WSNs. The methodology developed an ID technique utilizing Hybrid Tissue Growing Algorithm (HTGA) aimed at finding the anomalies presence cell and also the communication tissue structure to transmit the data-packets. The HADS protocol attained efficient performance regarding EC, packet delivery fraction, routing overhead, throughput, and also end-to-end delay.However, only restricted performance metrics were explored. It overlooked a few imperative performance metrics in exploring clustered methodologies, like communication cost. Table-3 explicates the examination of diverse techniques developed recently to administer the diverse attack types prevalent in WSN.

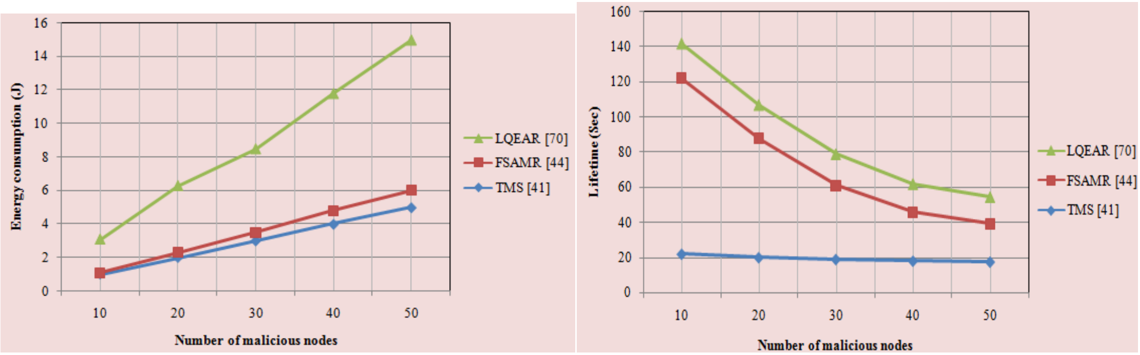
Table 3: Various frameworks for attack detection and security in WSN

Author	**Technique used**	**Attacks prevented**	**Results achieved**
M. S. Sumalath and V. Nandalal(2020)	The convolutional technique (CT) using convolutional codes	Malicious attacks	Attained minimal packet overhead, and also packet loss.
A. Ranjith Kumar and A. Sivagami(2020)	Hamming residue methodology aimed at WSN’s security improvement	Malicious attacks	Enhanced the confidentiality amidst the nodes, and detected the rival nodes easily.
V. R. SarmaDhulipala*et al.*(2013)	Effectual security procedure	The node replication attack, Sybil attack, and as well wormhole attack.	Achieved less computational cost and overhead.
P. N. Renjith(2018)	Security Localization Algorithm centred on distance vector-hop (DV-Hop)	Sybil attack	Whilst the number of beacon nodes is 50, the algorithm reduces the average localization error by 3%.
Author	Fuzzy logic (IADF)	Insider attacks	The PDR and residual energy attained by the IADF were greater.
K. Nirmal Raja and M. Marsaline-Beno(2014)	Fiege fiat shamir algorithm	DOS Attacks	PDR and throughput were incremented and also removed the malevolent nodes as of the network.
Yuping Zhou *et al.*(2020)	Distributed detection schemes: GDL and RMC	Node replication attacks	Lowest EC and largest communication overhead.
Sujesh P. Lal and P. M. Joe Prathap (2021)	Provenance centred defensive protocol	Malevolent selective forwarding attacks prevalent in multihop WSN.	The EC increments by 0.0628% in the technique
Rudra Pratap Ojha*et al.* (2019)	SEIQRV design aimed at WSN’s stability examination.	Malware Attacks	Only 13.55, 9.99, and 8.16 less % of SNs become affected in the design aimed at the diverse communication radius values.
Mojtaba Jamshidi (2020)	Sybil attack model with a	Sybil Attack	Detect Sybil nodes with

	distributed algorithm centred upon Received Signal Strength Indicator		99.8% accuracy and 0.008% false detection rate.
G. Keerthana et al. (2017)	Sequential probability ratio test (SPRT)	Spoofing and sniffing attacks	Attained moderate delay, greatest PDR, moderate drop ratio, greatest residual energy, and least overhead.

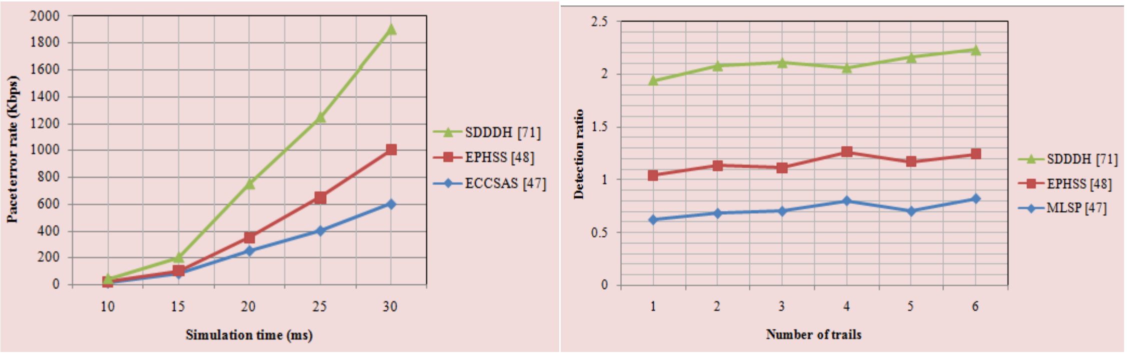
2.6 Results and Discussion

Herein, the outcomes of diverse trust-centred and routing protocols built aimed at attaining WSN's security are presented. The outcomes are offered centred on a few metrics. Fig-3 exhibits the outcomes attained by the diverse trust-centred protocols regarding EC and also lifetime. The protocols engaged aimed at analogy are TM Scheme (Swaminathan Ramesh, and Yaashuwanth C, 2020), Fuzzy-centred malevolent node detection and also security-aware multipath routing (FSAMR) (Ranjith Kumar A and Sivagami A, 2020), and Link Quality and Energy-Aware Routing (LQEAR) (Daojing He et al. 2013). EC is the extent of energy spend by every node in the transmission and lifetime is specified as the network's disconnection time as a reason of the failure of one or numerous SNs. The analogy performed by altering the number of malevolent nodes as of 10 to 50. The FSAMR (Ranjith Kumar A, and Sivagami A, 2020) protocol spends the least energy and highest lifetime aimed at all number nodes whilst analogized with (Swaminathan Ramesh, and Yaashuwanth C, 2020) and (Daojing He et al. 2013).



(a) (b)

Fig 3: EC and Lifetime of the trust-based mechanisms



(a) (b)

Fig 4: PER and detection accuracy of diverse techniques

Fig-4 (a) exhibits the packet error rate (PER) of the diverse routing protocols, like MLSP (Vidhya S, and Sasilatha T, 2018), EPHSS (YuvarajuM, and Pranesh K. A, 2020), and Secured Data Discovery and Dissemination centred upon Hash Tree (SDDDH) [71]. The EPHSS method achieved the lowest PER compared to SDDDH and MLSP. Whilst the technique's PER was less, which yields a decrementation of retransmission of error rate that instantaneously conserves nodal energy. Fig-4(b) exhibits the detection's accuracy of diverse techniques: MLSP, EPHSS, and also SDDDH. The '3' methodologies are assessed aimed at their capability and also potentiality of finding the insecure or else attacker nodes. Herein, the SDDDH achieved the highest detection accuracy whilst analogized to EPHSS and MLSP.

3. Conclusion and Discussion

Herein, recent methodologies' review aimed at WSN's security is offered. The protocols are surveyed centred on protocols utilized, outcomes achieved, advantages and demerits faced by the protocol developed. Wholly the survey of '5' diverse research subjects is offered: KM, authentication, trust, routing, and also ID-centred security techniques aimed at WSN. These topics' survey aids in the appropriate protocol's selection regarding their WSN application. However, there exist a few open problems aimed at proffering an effective security system (i.e.): i) providing a trust-centred solution aimed at every attack isn't possible. It as well suffers as of a greater cost, ii) a few restrictions of the KM procedure have overhead as of generating and also distributing keys after a little delay, probable message delay, iii) Availability and dependability are another prime concerns to the determined security solution that is centred on KM, authentication, and also TM, and iv) Cryptographic methodology suffers as of slow speed and is expensive within the resource constraint environment. So, there exists a future necessity to build a system aimed at security provisioning by pondering the limitations above. There exists a necessity aimed at an intelligent system comprising the mitigation of diverse attacks prevalent inside WSN, and also TM inside an unsecured environment utilizing stabilities, scalability, and as well overhead examination.

Declarations:

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Consent of publication: Not applicable.

Availability of data and materials: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests: The authors declare that they have no competing interests

Funding: This work has no funding resource.

Author's contributions: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by **VanitaVerma, Dr. Vijay Kumar Jha**. The first draft of the manuscript was written by **VanitaVerma** and all authors commented on previous versions of the manuscript.

All authors read and approved the final manuscript.

Acknowledgement: We thank the anonymous referees for their useful suggestions.

References

[1] Vinita Daiya, Jemimah Ebenezer, R, Jehadeesan, Security implementation in wireless Sensor network by RF signal obfuscation, Wireless Personal Communications. 2019;106(2):805-827. https://link.springer.com/article/10.1007/s11277-019-06191-7

[2] Alexey G. Finogeev, Anton A. Finogeev, Information attacks and security in wireless sensor networks of industrial SCADA systems, Journal of Industrial Information Integration. 2017;5:6-16, https,//doi.org/10.1016/j.jii.2017.02.002.

[3] Ghasem Farjamnia, Yusif Gasimov, Cavanshir Kazimov, Review of the techniques against the wormhole attacks on wireless sensor networks, Wireless Personal Communications. 2019;105(4):1561-1584. https://link.springer.com/article/10.1007/s11277-019-06160-0

[4] S. Sathees Babu, K. Balasubadra, Revamping data access privacy preservation method against inside attacks in wireless sensor networks, Cluster Computing. 2019;22(1):65-75. https://link.springer.com/article/10.1007%2Fs10586-018-1706-1

[5] Abdul Hamid Md, A.M. Jehad Sarkar, A group-based security scheme for wireless sensor networks, Annals of Telecommunications. 2012;67(9):455-469. http://dx.doi.org/10.1109/GLOCOM.2007.260

[6] P. Ilango, Secure authentication and integrity techniques for randomized secured routing in WSN, Wireless Networks. 2015;21(2):443-451. http://dx.doi.org/10.1007/s11276-014-0792-0

[7] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security, Journal of Ambient Intelligence and Humanized Computing, 2017;8(1):101-116. https://link.springer.com/article/10.1007/s12652-016-0345-8

[8] Ashok Kumar Das, A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks, Peer-to-peer Networking and Applications. 2016;9(1):223-244. http://dx.doi.org/10.1007/s12083-014-0324-9

[9] Deepak C. Mehetre, S. Emalda Roslin, Sanjeev J. Wagh, Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust, Cluster Computing. 2019;22(1):1313-

1328. https://link.springer.com/article/10.1007%2Fs10586-017-1622-9

[10] E. Suryaprabha, N.M. Saravana Kumar, Enhancement of security using optimized DoS (denial-of-service) detection algorithm for wireless sensor network, Soft Computing. 2020;24:10681–10691. https,//doi.org/10.1007/s00500-019-04573-4.

[11] Sunil Gupta, Harsh K. Verma, A.L. Sangal, Efficient security mechanism to counter the malicious attack in wireless sensor networks, CSI transactions on ICT. 2014;2(1):35-41. http://dx.doi.org/10.1007/s40012-014-0042-8

[12] Xiang Gu, Jin Wang, Jianlin Qiu, Zhengzheng Jiang, Self-recommendation mechanism in trust calculation among nodes in WSN, Wireless Personal Communications. 2017;97(3):3705-3723. https://link.springer.com/article/10.1007/s11277-017-4694-1

[13] Gautam M. Borkar, Leena H. Patil, Dilip Dalgade, Ankush Hutke, A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN a data mining concept, Sustainable Computing: Informatics and Systems. 2019;23:120-135, https,//doi.org/10.1016/j.suscom.2019.06.002.

[14] Aykut Karakaya, Sedat Akleylek, A survey on security threats and authentication approaches in wireless sensor networks, In 6th international symposium on digital forensic and security (ISDFS), IEEE. 2018. https://doi.org/10.1109/ISDFS.2018.8355381

[15] Bhawna Narwal, Amar Kumar Mohapatra, A Survey on security and authentication in wireless body area networks. Journal of Systems Architecture. 2020;113:1-57. https://doi.org/10.1016/j.sysarc.2020.101883

[16] Rosheen Qazi, Kashif Naseer Qureshi, Faisal Bashir, Najam Ul Islam, Saleem Iqbal, Arsalan Arshad, Security protocol using elliptic curve cryptography algorithm for wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing. 2021;12:547-566. https://link.springer.com/article/10.1007/s12652-020-02020-z

[17] A. Vaniprabha, P. Poongodi, Augmented lightweight security scheme with access control model for wireless medical sensor networks, Cluster Computing. 2019;22(5):12495-12505. https://link.springer.com/article/10.1007%2Fs10586-017-1669-7

[18] Chandra Sekhar Vorugunti, Bharavi Mishra, Ruhul Amin, Rakesh P. Badoni, Mrudula Sarvabhatla, Dheerendra Mishra, Improving security of lightweight authentication technique for heterogeneous wireless sensor networks, Wireless Personal Communications. 2017;95(3):3141-3166. https://link.springer.com/article/10.1007/s11277-017-3988-7

[19] Huei-Wen Ferng, Nguyen Minh Khoa, On security of wireless sensor networks, a data authentication protocol using digital signature, Wireless Networks. 2017;23(4): 1113-1131. https://link.springer.com/article/10.1007/s11276-016-1208-0

[20] Dheerendra Mishra, Pandi Vijayakumar, Venkatasamy Sureshkumar, Ruhul Amin, S.K. Hafizul Islam, Prosanta Gope, Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks, Multimedia Tools and Applications. 2018;77(14):18295-18325. https://link.springer.com/article/10.1007/s11042-017-5376-4

[21] Qi Jiang, Jianfeng Ma, Xiang Lu, Youliang Tian, An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks, Peer-to-peer Networking and Applications. 2019;8(6):1070-1081. http://dx.doi.org/10.1007/s12083-014-0285-z

[22] Mostafa H. Dahshan, Robust data authentication for unattended wireless sensor networks, Telecommunication Systems. 2019;66(2):181-196. https://link.springer.com/article/10.1007/s11235-017-0281-8

[23] Lina Yang, Shining Li, Zenggang Xiong, Meikang Qiu, HHT-based security enhancement approach with low overhead for coding-based reprogramming protocols in wireless sensor networks, Journal of Signal Processing Systems. 2019;89(1):13-25. https://link.springer.com/article/10.1007/s11265-016-1149-y

[24] Haitao Yu, Liejun Wang, A security-enhanced mutual authentication scheme with privacy protected in wireless sensor networks, Cluster Computing. 2019;22(3):7389-7399. https://link.springer.com/article/10.1007%2Fs10586-017-1575-z

[25] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security, Journal of Ambient Intelligence and Humanized Computing. 2017;8(1):101-116. https://link.springer.com/article/10.1007/s12652-016-0345-8

[26] Hong Yu, Jingsha He, Ting Zhang, Peng Xiao, Yuqiang Zhang, Enabling end-to-end secure communication between wireless sensor networks and

the Internet, World Wide Web. 2013;16(4):515-540. http://dx.doi.org/10.1007/s11280-012-0194-0

[27] Bo Sung Kim, Joo Seok Song,. Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks, EURASIP Journal on Wireless Communications and Networking. 2019;1:1-16. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1470-9

[28] Jangirala Srinivas, Dheerendra Mishra, Sourav Mukhopadhyay, Saru Kumari, Provably secure biometric based authentication and key agreement protocol for wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing. 2018;9(4):875-895. https://link.springer.com/article/10.1007/s12652-017-0474-8

[29] Jangirala Srinivas, Dheerendra Mishra, Sourav Mukhopadhyay, A mutual authentication framework for wireless medical sensor networks, Journal of medical systems. 2017;41(5) ()1-19. https://link.springer.com/article/10.1007/s10916-017-0720-9

[30] Amir Hosein Adavoudi-Jolfaei, Maede Ashouri-Talouki, Seyed Farhad Aghili, Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks, Peer-to-Peer Networking and Applications. 2019;12(1):43-59. https://link.springer.com/article/10.1007/s12083-017-0627-8

[31] Jian-Jun Yuan, An enhanced two-factor user authentication in wireless sensor networks, Telecommunication Systems. 2014;55(1),:105-113. https://link.springer.com/article/10.1007/s11235-013-9755-5

[32] Alma E Guerrero-Sanchez, Edgar A. Rivas-Araiza, Jose Luis Gonzalez-Cordoba, Manuel Toledano-Ayala, Andras Takacs, Blockchain mechanism and symmetric encryption in a wireless sensor network, Sensors. 2020;20(10):1-20. https://www.mdpi.com/1424-8220/20/10/2798#

[33] T. Lalitha, S. Jayaprabha, Mobility based key management security scheme for wireless sensor networks, Wireless Personal Communications. 2016;87(2):349-367. https://link.springer.com/article/10.1007/s11277-015-2872-6

[34] Simone Soderi, Acoustic-based security a key enabling technology for wireless sensor networks, International Journal of Wireless Information Networks. 2020;27(1):45-59. https://link.springer.com/article/10.1007/s10776-019-00473-4

[35] Khaled Hamouid, Salwa Othmen, Amine Barkat, LSTR, lightweight and secure tree-based routing for wireless sensor networks, Wireless Personal Communications. 2020;112:1479-15011. https://link.springer.com/article/10.1007/s11277-020-07111-w

[36] Yanrong Lu, Guangquan Xu, Lixiang Li, Yixian Yang, Anonymous three-factor authenticated key agreement for wireless sensor networks, Wireless Networks. 2019;25(4):1461-1475. https://link.springer.com/article/10.1007/s11276-017-1604-0

[37] Mohammad Sadegh Yousefpoor, Hamid Barati, DSKMS, A dynamic smart key management system based on fuzzy logic in wireless sensor networks, Wireless Networks. 2020;26(4):2515-2535. https://link.springer.com/article/10.1007/s11276-019-01980-1

[38] Tianshu Wang, Kongfa Hu, Xichen Yang, Gongxuan Zhang, Yongli Wang, A trust enhancement scheme for cluster-based wireless sensor networks, The Journal of Supercomputing. 2019;75(5):2761-2788. https://link.springer.com/article/10.1007/s11227-018-2693-y

[39] Tong Zhang, Lisha Yan, Yuan Yang, Trust evaluation method for clustered wireless sensor networks based on cloud model, Wireless Networks. 2018;24(3):777-797. https://link.springer.com/article/10.1007/s11276-016-1368-y

[40] Xueqiang Yin, Shining Li, Trust evaluation model with entropy-based weight assignment for malicious node’s detection in wireless sensor networks, EURASIP Journal on Wireless Communications and Networking. 2019;1:1-10. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1524-z

[41] Swaminathan Ramesh, C. Yaashuwanth. Enhanced approach using trust based decision making for secured wireless streaming video sensor networks, Multimedia tools and applications. 2020;79(15):10157-10176. https://link.springer.com/article/10.1007/s11042-019-7585-5

[42] Osama Al Farraj, Ahmad AlZubi, Amr Tolba, Trust-based neighbor selection using activation function for secure routing in wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing. 2018. https,//doi.org/10.1007/s12652-018-0885-1.

[43] M.S. Sumalatha, V. Nandalal, An intelligent cross layer security based fuzzy trust calculation

mechanism (CLS-FTCM) for securing wireless sensor network (WSN), Journal of Ambient Intelligence and Humanized Computing. 2020;12:1-15. https://link.springer.com/article/10.1007/s12652-020-01834-1

[44] A. Ranjith Kumar, A. Sivagami, Fuzzy based malicious node detection and security-aware multipath routing for wireless multimedia sensor network, Multimedia Tools and Applications. 2020;79:14031-14051. https://link.springer.com/article/10.1007/s11042-020-08631-0

[45] V.R. Sarma Dhulipala, N. Karthik, R.M. Chandrasekaran, A novel heuristic approach based trust worthy architecture for wireless sensor networks, Wireless personal communications. 2013;70(1):189-205. https://link.springer.com/article/10.1007/s11277-012-0688-1

[46] P.N. Renjith, Towards secure data forwarding with ANFIS and trust evaluation in wireless sensor networks, Wireless Personal Communications. 2020;114(1):765-781. https://link.springer.com/article/10.1007/s11277-020-07392-1

[47] S. Vidhya, T. Sasilatha, Secure data transfer using multilayer security protocol with energy power consumption AODV in wireless sensor networks, Wireless Personal Communications. 2018;103(4):3055-3077. https://link.springer.com/article/10.1007/s11277-018-5994-9

[48] M. Yuvaraju, K.A. Pranesh, Energy proficient hybrid secure scheme for wireless sensor networks, Wireless Personal Communications. 2020;117:747–767. https,//doi.org/10.1007/s11277-020-07895-x.

[49] Jie Cui, Lili Shao, Hong Zhong, Yan Xu, Lu Liu, Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks, Peer-to-Peer Networking and Applications. 2018;11(5):1022-1037. https://link.springer.com/article/10.1007/s12083-017-0581-5

[50] Hiren Kumar Deva Sarma, Avijit Kar, Rajib Mall, A hierarchical and role based secure routing protocol for mobile wireless sensor networks, Wireless Personal Communications. 2016;90(3):1067-1103. https://link.springer.com/article/10.1007/s11277-016-3379-5

[51] R.S. Raghav, Kalaipriyan Thirugnansambandam, Dinesh Kumar Anguraj, Beeware routing scheme for detecting network layer attacks in wireless sensor networks, Wireless Personal Communications. 2020;112(4):2439-2459. https://link.springer.com/article/10.1007/s11277-020-07158-9

[52] Michele Tortelli, Alessandra Rizzardi, Sabrina Sicari, Luigi Alfredo Grieco, Gennaro Boggia, Alberto Coen-Porisini, S2 DCC, Secure selective dropping congestion control in hybrid wireless multimedia sensor networks, Wireless Networks. 2018;24(1):309-328. http://dx.doi.org/10.1007/s11276-016-1332-x

[53] Jayanthi Ramasamy, John Singh Kumaresan, Image encryption and cluster based framework for secured image transmission in wireless sensor networks, Wireless Personal Communications. 2020;112:355-1368. https,//doi.org/10.1007/s11277-020-07106-7.

[54] P. Brindha, A. Senthilkumar, Data dependability based bimodal encryption scheme for distributed routing in wireless sensor networks, Peer-to-Peer Networking and Applications. 2019;13:1142-1151. https,//doi.org/10.1007/s12083-019-00813-4.

[55] Ashfaq Hussain Farooqi, Farrukh Aslam Khan, Jin Wang, Sungyoung Lee, A novel intrusion detection framework for wireless sensor networks, Personal and ubiquitous computing. 2013;17(5):907-919. https://link.springer.com/article/10.1007/s00779-012-0529-y

[56] Xin Xiao, Ruirui Zhang, Study of immune-based intrusion detection technology in wireless sensor networks, Arabian Journal for Science and Engineering. 2017;42(8):3159-3174. https://link.springer.com/article/10.1007/s13369-017-2426-1

[57] Somnath Sinha, Aditi Paul, Neuro-fuzzy based intrusion detection system for wireless sensor network, Wireless Personal Communications. 2020;114(1):835-851. https://link.springer.com/article/10.1007/s11277-020-07395-y

[58] C. Umarani, S. Kannan, Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network, Peer-to-Peer Networking and Applications. 2020;13(3):752-761. https://link.springer.com/article/10.1007/s12083-019-00781-9

[59] Turki Ali Alghamdi, Convolutional technique for enhancing security in wireless sensor networks against malicious nodes, Human-centric Computing and Information Sciences. 2019;9(1):1-10. http://dx.doi.org/10.1186/s13673-019-0198-1

[60] Majid Alotaibi, Security to wireless sensor networks against malicious attacks using Hamming residue method, EURASIP Journal on Wireless Communications and Networking. 2019. https://doi.org/10.1186/s13638-018-1337-5

[61] T.D. Ovasapyan, Denis V. Ivanov, Security provision in wireless sensor networks on the basis of the

trust model, Automatic Control and Computer Sciences. 2018;52(8):1042-1048. https://link.springer.com/article/10.3103/S0146411618080205

[62] Shi Dong, Xin-gang Zhang, Wen-gang Zhou, A security localization algorithm based on DV-hop against sybil attack in wireless sensor networks, Journal of Electrical Engineering & Technology. 2020;15(2):919-926. https://link.springer.com/article/10.1007/s42835-020-00361-5

[63] Ashwinth Janarthanan, Dhananjay Kumar, R. Remo Antony, C.B. Divya Parvathe, IADF security, Insider attack detection using fuzzy logic in wireless multimedia sensor networks, Soft Computing. 2020;24(4):1-10. https://link.springer.com/article/10.1007/s00500-020-04764-4

[64] K. Nirmal Raja, M. Marsaline Beno, On securing wireless sensor network-novel authentication scheme against DOS attacks, Journal of medical systems. 2014;38(10):1-5. https://link.springer.com/article/10.1007/s10916-014-0084-3

[65] Yuping Zhou, Zhenjie Huang, Juan Wang, Rufeng Huang, Dongmei Yu, An energy-efficient random verification protocol for the detection of node clone attacks in wireless sensor networks, EURASIP Journal on Wireless Communications and Networking. 2014;1:1-12. http://dx.doi.org/10.1186/1687-1499-2014-163

[66] Sujesh P. Lal, P.M. Joe Prathap, A provenance based defensive technique to determine malevolent selective forwarding attacks in multi-hop wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing. 2020;12(5):5589–5597 https://link.springer.com/article/10.1007/s12652-020-02079-8

[67] Rudra Pratap Ojha, Pramod Kumar Srivastava, GoutamSanyal, Nishu Gupta, Improved model for the stability analysis of wireless sensor network against malware attacks, Wireless Personal Communications. 2021;116(3):2525-2548. https://link.springer.com/article/10.1007/s11277-020-07809-x

[68] Mojtaba Jamshidi, Ehsan Zangeneh, Mehdi Esnaashari, Aso Mohammad Darwesh, Mohammad Reza Meybodi, A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it, Wireless Personal Communications. 2019;105(1):145-173. https://doi.org/10.1007/S11277-018-6107-5

[69] G. Keerthana, P. Anandan, N. Nandhagopal, Enhancing the robustness and security against various attacks in a scale, free network, Wireless Personal Communications, 2020;117:3029–3050. https://link.springer.com/article/10.1007/s11277-020-07356-5

[70] Shailendra Aswale, Vijay R. Ghorpade, LQEAR, link quality and energy-aware routing for wireless multimedia sensor networks, Wireless Personal Communications. 2017;97(1):1291-1304. https://doi.org/10.1007/s11277-017-4566-8

[71] Daojing He, Sammy Chan, Shaohua Tang, Mohsen Guizani, Secure data discovery and dissemination based on hash tree for wireless sensor networks, IEEE transactions on wireless communications. 2013;12(9):4638-4646. https://doi.org/10.1109/TWC.2013.090413.130072

Biography

Ms. Verma received her M.Sc. Degree from Indian School of Mines, Dhanbad currently known as ISMIIT in Mathematics and Computing in 2011. She has 7 years of work experience in IT industry. In present she is pursuing her Ph.D degree in Computer science from Birla Institute of Technology, Mesra, Ranchi. Her current research interest includes Big Data analytic, Data Mining, and Network Security.

Mr. Jha is currently an Associate Professor in Birla institute of Technology, Mesra, Ranchi. He had Joined the institution on 3rd Apr. 2001. His research areas are Network security, Data mining, Big data Analysis.