International Journal on Emerging Technologies 14(1): 36-41(2023)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Survey on Secure Trust based Routing in WSN

Hemavathi Patil[1*] and Vishwanath Tegampure[2]
[1]Research Scholar, Department of ISE,
Guru Nanak Dev Engineering College, Bidar (Karnataka), India.
[2]Professor, Department of ECE
Bheemanna Khandre Institute of Technology, Bhalki (Karnataka), India.

(Corresponding author: Hemavathi Patil)*
(Received 15 February 2023, Revised 18 April 2023, Accepted 30 April 2023)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless sensor networks (WSNs) are always plagued by serious security issues. A number of trust-based routing methods have been developed, and they are the key to improving wireless network effectiveness. However, due to unreliable wireless communication networks, they remain have significant drawbacks like low energy reserves, vulnerability to physical capture, and insufficient security against numerous attacks. Because of the built-in vulnerability of WSN to assaults, security is a necessity in WSN and is incredibly difficult to provide. A WSN node that is involved must transport data to nearby nodes to avoid a disaster in the event of a node attack. Recently, trust mechanisms have increasingly been viewed as the best method for reducing security issues in WSN. The goal of this study is to examine several Security routing methods and techniques for wireless sensing connections that are already in use and rely on trust. The technique, trust metric, benefits, drawbacks, and complexity of the idea behind the current trust mechanism are all examined. The security resilience of different trust types towards attacks are also examined in the final stage.

Keywords: WSN, Security, Routing, Energy, Malicious nodes, Trust Nodes.

I. INTRODUCTION

A WSN is made up of battery-operated sensor nodes with very minimal computing power [1]. It comprises an extensive variety of uses, such as tracking the environment, buildings and urban monitoring, manufacturing operations, individual healthcare, and protection of the homeland. Their rising use is mostly due to their many benefits, including self-organizing, inexpensiveness, and wireless functioning. Yet, these benefits raise security concerns [2]. To achieve the random deploy demand, the nodes must collaborate together to do specific networking activities, which creates fresh vulnerabilities. WSNs are subject to breaches of privacy because of their wireless functioning, and the inexpensive nature of the nodes is closely linked to their limited processor, memory, and energy capacities, which restricts the range of features that can be added to mitigate security breaches. Because of the way routing works in WSN, safe routing becomes increasingly difficult. Because the WSN doesn't have an infrastructure, nodes must work together to cooperatively route traffic. So, in a WSN, a router is just any node in the network that provides forwarding services.

Recent susceptible assaults carried out on multiple nodes by intruders have made WSN an unsecured situation [3]. Attacks at the routing levels include denial of service (DoS), spoofing, Sybil, black hole, and Sybil-like attacks. The DoS attacks are the most significant security risk of all of them. In order to protect the WSN, several academics are striving to create a new secure routing protocol. This paper proposes a novel energy-efficient routing method that conserves energy by detecting and averting security assaults. Whenever nodes engage in fraudulent activities, the issue with WSN's energy usage arises. As a result, authors discovered that stopping harmful activity can conserve energy in sensor nodes. It is important for providing a secured channel in a manner that ensures the suggested pathway can be recognized by calculating the trust, which determines the truthfulness of the contributing nodes, with the goal to enable reliable communication. The term "trust" refers to the degree of trust that neighborhood nodes have in their ability to send and receive messages safely during routing. Assessing trust among neighborhood nodes is essential to preventing security vulnerabilities in WSN. In accordance with direct and indirect trust or acceptance standards, trust values are assessed [4].

Direct trust refers to interactions among neighboring nodes that are both profitable and failing. Referral trust or indirect trust is the act of recommending one node to another. The choice to choose the optimum route to reach the goal is determined in accordance with the trust numbers, however, trust in a specific node changes with time, and the trust values themselves might rise or fall. The only legitimate nodes used for transmission are those that are determined by assessing trust. The overall trust of the nodes, which is derived from direct trust and indirect trust, is used to identify the specific assaults.

For efficient communication, several different protocols for routing are employed, although they are only beneficial for sending data at reduced energy costs from one particular node to a different one [28]. Only trust-based or energy-efficient routing ought to be offered by

the protocols employed for successful communication. A routing system that integrates a node's perception of an individual router's behavior into its routing choice is known as a trust-aware routing mechanism [5]. The trust measure, which quantifies this judgment, is used. Trust metrics are used to determine the pathway from origin to target. Routing that is trust-aware is crucial for safeguarding network assets from irrational use, safeguarding network efficacy from deterioration, and securing data that has been collected. The majority of WSN applications, such as those used in the military and healthcare carry and send highly sensitive information. Behaving improperly nodes contaminated with WSN misroute data packets to the incorrect destination, resulting in incorrect data, or fail to forward messages to the correct destination, resulting in the loss of data. A trust-aware routing method will guarantee the delivery of data, preserve the importance of transmitted data, and safeguard data interchange [6]. Nevertheless, there are some significant issues with the conventional trust-based routing methods. The trust-based techniques address the innate threats in wireless networks, but they also introduce some additional hazards that require careful attention. Additionally, the majority trust instances do not take into account the uniqueness of trust statistics when developing algorithms for routing and the current trust-based routing algorithms have certain boundaries such as reliance on a specific routing method, which renders the safety features useless if the network's algorithm for routing is altered.

Because of the way routing works in WSN, secure routing becomes increasingly difficult. Because the WSN does not have a network structure, nodes must work together to cooperatively route information. The predominant goals for secure routing consists data confidentiality, data integrity, data availability and secure packet delivery.

So, in a WSN, a router is just any node that provides routing services. In order to route the message in a highly secure manner, this "any node" should be used. To make the best routing choice, we must first comprehend the security objectives we are trying to achieve. A routing technique known as a "trust aware routing protocol" allows a node to factor in its perception of a prospective router's behavior when making a routing choice. The trust measure, which quantifies this judgment, is used. A router's anticipated behavior, such as forwarding a packet when it gets it from a prior node, should be reflected in the trust metric. The measurement of trust is a challenge in and of itself since it involves a number of operational procedures, including watching node behavior, communicating expertise and views across nodes, and modelling the learned insights and shared information to reflect node trust levels. A trusted system is a system which performs these operations and finally outputs a "rating" or a trust value on nodes.

The common attacks which may encounter in the wireless networks are, (i) A black hole attack when a malevolent node throws away all the packets it ought to forward. (ii) A grey hole attack, whereby an intruder removes some packet types and sends a portion of them. (iii) A sinkhole attack is when a hacked node pretends to be a sink node and draws almost all of the bandwidth from a certain location. (iv) Information packets collected in one area of the network might get penetrated by two rivals and recalled in another region over a minimal latency connection in a wormhole attack. (v) A hostile node manipulates a received message in a message tampering attack while passing it across other nodes [7]. (vi) In a rank attack, the rogue node lures users in by promoting its fictitious rank rating. Significantly alter the network architecture, add routing loops and non-optimal pathways. As a result, safe routing is crucial to ensuring network operation when confronted with of selfishness or malevolent nodes, and numerous algorithms for routing have been enacted periodically to this end. Nevertheless, the majority of the aforementioned routing protocols depend upon authentication approaches and cryptographic fundamentals that are inappropriate for WSNs.

II. RELATED WORK

In [8] author proposed a security-conscious ring cluster routing method. The routing process is dependent on a number of variables, like distance, energy, and trust characteristics. In this instance, both the direct and indirect trust evaluations are included in the trust criteria. As a result, the network's lifespan is increased in an efficient way. This work presents a novel Self-Adaptive Deer Hunting Optimisation (SA-DHO), which is important in the selection of the neighbours as ring nodes. In reference to several metrics, the recommended method's effectiveness is eventually shown.

In [9] authors mentioned that, in order for people to communicate with one another on a regular basis, technological innovation in networking is essential. The most crucial problem with wireless networks is security. In recent years, security has been provided by behavior analysis using trust and reputation methods. The current works, nevertheless, fall short in their ability to reliably secure wireless networks. The authors of this research suggest using the intelligent dynamic trust model (IDT) to provide security for wireless networks. For safe routing in wireless networks, this paradigm combines beta reputational trust with dynamic trust.

In [10] the author proposed the network's backbone nodes in the designs suggested are distributed across the system utilizing the secure trust-based group key generation (STGG) technique. The authors use the elimination-related approach to create a secure clustering process. The criteria used for node optimization are used to determine the cost estimate. The dynamic key for the data transfer is estimated using it. The clustering phase needs to be protected since the restrictions utilized for clustering formation are employed as a supplemental during dynamic key generation. Secured cluster retention is carried out whenever a node moves between clusters, and secured route identification is used within clusters when information has to be broadcast from the the sources to sink node. The suggested system is more secure and has less network connection overhead.

In [11] author depicted that the wide deployment of the sensors makes them susceptible to security concerns. Additionally, security is not a factor in the majority of routing methods. In the previous study, a number of security-related techniques were taken into consideration, including detecting intrusions, network firewalls, trust governance, and management of keys.

The trust management provides increased security among them. In order to address security problems, writers adopted the secure trust-based enhanced LEACH routing (STELR) mechanism in this research. In this case, the emperor penguin optimization technique is utilized to pick the cluster head to perform data aggregation, while STELR is employed for enabling security for routing. It can also enable secure interactions by determining whether a node is trustworthy. Comparing the proposed methodology to current methods like LEACH and SDILR protocols, it performs better. Works doesn't shown the energy parameter and lifespan criteria.

In [12] author suggested that, to address security issues, this study suggests a brand-new trust-based secure and energy-efficient routing protocol (TBSEER). Using adaptive direct, indirect, and energy trust values, TBSEER determines an extensive trust value, that can withstand attacks from black holes, selective forwarding, sinkholes, and hello floods. Additionally, harmful nodes are quickly identified by using the volatilized aspect and adaptable penalty mechanisms. In order to further decrease the energy usage brought on by repetitive computations, the nodes just must determine the direct trust value, and the Sink obtains the indirect trust rating. Lastly, depending on the total trust value, the cluster heads identify the safest multi-hop paths, actively preventing wormhole attacks.

In [13] author mentioned that, over the years, a number of routing models have been developed suggested to create a secure routing. An innovative routing algorithm for wireless datagram networking called Greedy Perimeter Stateless Routing (GPSR) generates greedy choices for forwarding utilizing only knowledge of a router's close neighbors in the network configuration. As the total number of network endpoints grows, it scales faster in the per-router context than shortest-path and ad hoc routing algorithms. Nevertheless, no protection against assaults can be offered by this process.

In article [14], a secure trust based key management (STKF) routing paradigm is presented. The method creates a safe trusted pathway based on the node-to-node connections that have occurred in both the past and present. The selected path is subsequently updated by removing any fraudulent or compromised devices that exist on the path, if any, and a separate connection is created using the "q" combined random key pre-distribution scheme (RKPS) among each pair of nodes in the chosen route to guarantee the transmission of data from starting point to the final location. The suggested routing strategy's effectiveness is contrasted with that of the trust-aware secure routing framework (TSRF). The findings show that STKF offers an efficient method for determining a secure route that is more reliable than TSRF and prevents data dropping, hence improving the data delivery ratio. Additionally, the suggested approach reduces the distance needed to go to the target, effectively utilizing the available resources. The energy requirement is quite high in this proposed methodology.

To increase the level of safety of WSNs, trust-based routing became popular in the last few years which is explained in [15]. By adding a trust-based technique to the current Dynamic Source Routing (DSR), a safe DSR protocol is built for mobility networked sensors. The DSR protocol's built-in characteristics are used by the trust model to calculate and estimate the corresponding levels of trust across nodes. The foundation of the protocol being discussed is the trust update interval (TUI), which establishes the amount of time the sending nodes have to endure following sending a packet before updating a trust value according to the response it receives. The method can, however, defend against specific kinds of assaults.

In [16] a trust-aware location-based routing protocol was developed to facilitate large-scale WSN installations while simultaneously defending the WSN from routing threats. The suggested technique has been used with cutting-edge sensor nodes for a practical test bed and has proven to effectively identify and avoid rogue nodes. The writer has here focused on the evaluation of the cost of execution as well as the insights discovered during the conception, execution, and validation processes.

In [17] author proposed a reliable trust-aware routing system for dynamic WSNs and it was created and implemented by TARF. The proposed initiative offers a reliable, time- and energy-efficient approach. The robustness of TARF is confirmed by rigorous assessment involving both implementations and practical testing on a broad scale. Most significantly, TARF demonstrates resilience against certain destructive assaults built out of identification falsification.

In [18] author introduces a security-aware ring cluster routing approach. The routing process is dependent on a number of variables, such as distance, energy, and trust characteristics. In this article, both direct and indirect trust evaluations are included in the trust criteria. As a result, the network's lifespan is increased in a secure way. This work presents a novel Self-Adaptive Deer Hunting Optimisation (SA-DHO), which is essential for the neighbors as ring nodes. In reference to several metrics, the recommended method's advantage is eventually shown in this article.

In [18] author mentioned that the security is a key component of WSN, methods of routing must take security into account. Trust management, detection of attacks, firewalls, and the handlings of keys are among the several security measures taken. Comparing them to other security measures, trust management may amongst them offer increased safety. In order to recognize fraudulent activity in WSN efficiently an improved secure routing method referred to energy-aware trust-based secure routing technique is put forward in this article. The method uses a decision tree approach with spatiotemporal constraints to choose the best route. It has been demonstrated through testing that this suggested trust-based routing method outperforms previous techniques significantly.

In [19] author described that, with the aid of efficient clustering algorithms for confirming the nodes throughout the movement, a dynamic keying solution has been presented for securing the communication network. Using this method, secure network communication is made possible by dynamically created keys. The same key is unable to be utilized by intruders to breach the network even if the earlier used codes are taken by the hackers. An essential component of offering safe communication trusts a node. The research area of social science is where the word "trust" originated. The notion of trust is currently being used by scholars on social

networking platforms like Facebook, Twitter, LinkedIn, and others. Trust facilitates dependable communication. The word "consensus" often refers to conformity with the conclusion or conclusion made by a group acting collectively [20]. A novel socio psychological trust model with consensus awareness is given. In group-oriented wireless sensor networks, the consensus method specifies ways to reach specific locations, acquire velocity, and achieve orientation, among other things. The adjacency matrix is created in a group-based WSN in order to link nearby nodes. A weighted Laplacian matrix is used to preserve the framework of the sensor system. The suggested paradigm was primarily created to establish confidence between nodes. This is accomplished by incorporating the three components of ABI. A represents for aptitude, B for goodness, and I for integrity. This paradigm focuses on all three of the main trust factors—A, B, and I—and is both straightforward and effective.

III. IMPORTANCE OF SECURE TRUST BASED ROUTING

In a WSN, secure trust aware routing is crucial for safeguarding collected data as well as preventing network reliability deterioration and irrational resource use. The majority of WSN applications, such as those used in the military and healthcare, transport and send highly sensitive information. A WSN network with errant nodes might misroute messages and send them to the incorrect destinations, resulting in inaccurate information, or it can fail to direct messages to their intended destinations, resulting in an interruption of data. These crucial applications may be extremely vulnerable to these assaults. A trust-aware secure routing method can ensure the transmission of information, safeguard data sharing, and retain and defend the value of the transmitted information.

Efficiency can also be harmed by node misbehavior. For instance, non-forwarding attacks reduce system performance because messages are repeatedly sent but are not received. The handling of additional packets may be delayed as a result of denial-of-service attacks as certain router nodes are going to be engaged defending against the assault. Because of non-forwarding attacks, an attacked WSN network can be divided into separate segments that are unable to interact with one another. This creates a need for more sensors or for a different node placement in order to restore network access. Although this is somewhat costly, it may be prevented by using a solid secure routing approach. The resources of the network are additionally impacted by malfunctioning nodes. The DoS attacks, for instance, have an impact on the accessibility of resources, whether one utilizes an annoyed node as an asset for forwarding or the provision of information itself. Additionally, this assault makes the targeted nodes expend extra energy on packet receipt and execution. The degree of protection given by trust awareness of the routing process in WSN has an immediate impact on its data quality and the efficiency of the network.

IV. SECURE TRUST BASED ROUTING MECHANISMS AND COMPARISIONS

This section focuses on several trust-centered secrecy routing approaches. Trust is often demanded from every aspect, all over, and at all times. Likewise, WSN is also intended to earn people's confidence. For security-related problems in WSN, symmetric and asymmetric cryptographic algorithms offer diverse solutions. If a malicious node has the necessary key, it can appear to be a valid node, earning the trust of other legitimate nodes. Additionally, it becomes necessary to approve each and every node that is installed in the WSN. Uncertainty can be effectively managed if two connected sensor nodes may develop confidence in one another. The trust management method suggested did not take reputations or trust into account. Information collecting at different levels and risk management should have been addressed more in the BS level of trust [21]. The trust models can be divided into two types, data trust model and node trust model [22].

The basic building block of a data network is information. It holds true for WSNs as well since the information from one sensor node needs to be transferred to other nodes. WSN's core functions are data collection, processing, and transfer. Although WSN's transmission of data process is susceptible to several threats. Attacks like eavesdropping, alteration, impersonation, etc., become simply conceivable if the wireless link is exploited. Security at the data level and protection at the level of data trust so become significant phenomena.

Typically, node trust models may be divided into two categories: 1) The centralized node trust paradigm, and 2) the distributed node trust paradigm. To calculate the value of the parameter of confidence for the specifying sensor node, a middle unit designated Base Station (BS) is selected to be believed in the centralized trust model. Every sensor node in the distribution trust model assesses its own trust value. Table 1 compares some of the recent articles published on secure routing along with their research gaps.

Table 1: Trust based methods for secure routing- Comparisons.

Reference	Domain	Techniques used	Trust Metrics	Attacks	Research Gap
[23]	ML-TRUST	Multilevel and subjective-objective based TMS	Subjective trust, objective trust and recommended trust	Multiple attacks	Only communication trust is taken into account when estimating trust. Trust-building and sharing are not taken into account. additionally, data trust is not taken

					into account when estimating trust.
[24]	Data Trust	Adaptive and dual Data-Communication Trust scheme	adaptive trust function, Communication trust	untrustworthy nodes	Only data and communication trust are taken into account when estimating trust.
[9]	Trust Model	Intelligent dynamic trust model and intelligent beta reputation	Dynamic trust value, Direct Trust, reputation values	Node authentication	Research preferred for security but lags in lifespan as energy parameter is not considered.
[25]	RPL attacks	Multidimensional and dynamic trust model	QoS, Contextual Information	Blackhole and Rank	Doesn't use the network's impact on sink nodes' mobility into account.
[26]	RPL attacks	fuzzy logic-based approach.	Feedback, observation, node transactions	Sybil and Rank	does not take into account the mobility of nodes; a considerable packet loss probability; E2E interruptions, utilization of energy, and coordinated attacks haven't been assessed; Does not take into account the ambiguity of suggestions
[27]	Wireless Routing attacks	inclusion of dummy packets	Route trust, direct trust and indirect trust	Packet dropping attacks	Significant overhead is produced by inserting a dummy packet into networks. Other specific attacks (RPL) have not been taken into account.

V. TRUST INDEX CALCULATIONS

The trust index is created by combining the trust measures with the specified values. Historical analysis findings receive less weight (0.10) while present trust levels are provided greater weight (0.18). Since they depends on the nodes' most recent assessments, their achievement rate, power, position, mobility, and suggested trust are each assigned a corresponding weight of 0.18. While the past assessment receives a lower weighting of 0.10 since it relies on prior actions, it is still crucial to take this into account of it in order to build confidence gradually rather than abruptly. The scores of aggregated trust range from 0 to 1. Trust index evaluates trust ratings using the idea of a fuzzy threshold-based approach. i3 tuple has been used as a threshold. For routing, the nodes with greater trust levels are chosen first. Table for trust index is as shown in Table 2.

Table 2: Trust index calculations.

Trust Index	Rating	Range Values
i1	Zero-Trust	0 to 0.20
i2	Poor-Trust	0.21 to 0.45
i3	Fair-Trust	0.46 to 0.70
i4	Good-Trust	0.71 to 0.90
i5	Full-Trust	0.91 to 1

VI. CONCLUSION AND FUTURE SCOPE

An efficient system for identifying unauthorized nodes and their behaviors in WSN is included in Trust Models. The neighboring nodes can utilize the trust knowledge to avoid the misbehaving node after it has been identified as such. The paper surveys the recent advancements in secure trust based routing in WSN. Various parameters have been considered for the trust based secure routing. The trust based mechanisms, comparisons, trust index calculations have been depicted in this paper.

The paper can be extended by considering the trust based routing for multimedia content as well. This paper describes the work for physical information or static content. In future, the security can also be given to large video, audio and image files.

Acknowledgement. We thank Visvesvaraya Technological University, Belagavi for providing necessary information in writing the article.
Conflict of Interest. None.

REFERENCES

[1]. Senouci, M. R., & Mellouk, A. (2019). A robust uncertainty-aware cluster-based deployment approach for WSNs: Coverage, connectivity, and lifespan. *Journal of Network and Computer Applications*, *146*, 102414.

[2]. Sharmila, P., & Priyadharson, A. S. M. (2019). A cluster-based secured data transmission protocol for efficient data gathering in WSN. *International Journal of Vehicle Information and Communication Systems*, *4*(4), 331-343.

[3]. Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V., & Amiri, I. S. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, *11*, 4995-5001.

[4]. Palanisamy, S., Sankar, S., Somula, R., & Deverajan, G. G. (2021). Communication trust and energy-aware routing protocol for WSN using DS theory. *International Journal of Grid and High Performance Computing (IJGHPC)*, *13*(4), 24-36.

[5]. Wang, T., Hu, K., Yang, X., Zhang, G., & Wang, Y. (2019). A trust enhancement scheme for cluster-based wireless sensor networks. *The Journal of Supercomputing*, *75*, 2761-2788.

[6]. Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, *110*, 1637-1658.

[7]. Duan, J., Yang, D., Zhu, H., Zhang, S., & Zhao, J. (2014). TSRF: A trust-aware secure routing framework in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *10*(1), 209436.

[8]. Sumesh, J. J., & Maheswaran, C. P. (2023). Energy Efficient Secure-Trust-Based Ring Cluster Routing in Wireless Sensor Network. *Journal of Interconnection Networks*, *23*(02), 2250004.
[9]. Dheepak, T. (2021). Enhance The Wireless Network Security With A Secure Trust Routing Approach. *Webology (ISSN: 1735-188X)*, *18*(2).
[10]. Sabena, S., Sureshkumar, C., Sai Ramesh, L., & Ayyasamy, A. (2021). Secure Trust-Based Group Key Generation Algorithm for Heterogeneous Mobile Wireless Sensor Networks. In *Inventive Computation and Information Technologies: Proceedings of ICICIT 2020* (pp. 127-141). Springer Singapore.
[11]. Rajesh, L., & Mohan, H. S. (2022). EPO Based Clustering and Secure Trust-Based Enhanced LEACH Routing in WSN. In *Sustainable Communication Networks and Application: Proceedings of ICSCN 2021* (pp. 41-54). Singapore: Springer Nature Singapore.
[12]. Hu, H., Han, Y., Yao, M., & Song, X. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. *IEEE Access*, *10*, 10585-10596.
[13]. Karp, B., & Kung, H. T. (2000, August). GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 243-254).
[14]. Kaur, J., Gill, S. S., & Dhaliwal, B. S. (2016). Secure trust based key management routing framework for wireless sensor networks. *Journal of Engineering*, *2016*.
[15]. Samundiswary, P., & Dananjayan, P. (2010). Secured reactive routing protocol for mobile nodes in sensor networks. *WSEAS Transactions on Communications*, *9*(3), 216-225.
[16]. Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos, C., & Besson, L. (2010). Design and implementation of a trust-aware routing protocol for large WSNs. *International Journal of Network Security & Its Applications (IJNSA)*, *2*(3), 52-68.
[17]. Samundiswary, P., & Dananjayan, P. (2010). Performance analysis of trust based AODV for wireless sensor networks. *international journal of computer applications*, *4*(12), 6-13.
[18]. Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., & Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications*, *105*, 1475-1490.
[19]. Kesavan, V. T., & Radhakrishnan, S. (2016). Cluster based secure dynamic keying technique for heterogeneous mobile wireless sensor networks. *China Communications*, *13*(6), 178-194.
[20]. Rathore, H., Badarla, V., & Shit, S. (2016). Consensus-aware sociopsychological trust model for wireless sensor networks. *ACM Transactions on sensor networks (TOSN)*, *12*(3), 1-27.
[21]. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*, *80*(3), 602-617.
[22]. Prabhu, S., & EA, M. A. (2020). Trust based secure routing mechanisms for wireless sensor networks: A survey. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1003-1009). IEEE.
[23]. Zhang, B., Huang, Z., & Xiang, Y. (2014). A novel multiple-level trust management framework for wireless sensor networks. *Computer Networks*, *72*, 45-61.
[24]. Talbi, S., Koudil, M., Bouabdallah, A., & Benatchba, K. (2017). Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. *Telecommunication Systems*, *65*, 605-619.
[25]. Hashemi, S. Y., & Shams Aliee, F. (2019). Dynamic and comprehensive trust model for IoT and its integration into RPL. *The Journal of Supercomputing*, *75*, 3555-3584.
[26]. Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Generation Computer Systems*, *93*, 860-876.
[27]. Sakthivel, T., & Chandrasekaran, R. M. (2018). A dummy packet-based hybrid security framework for mitigating routing misbehavior in multi-hop wireless networks. *Wireless Personal Communications*, *101*(3), 1581-1618.
[28]. Belagali, R., Anusha, A. M., & Sangulagi, P. (2015, October). Energy-efficient secure routing and aggregation in military sensor network using multi-agent approach. In *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)* (pp. 286-292). IEEE.

How to cite this article: Hemavathi Patil and Vishwanath Tegampure (2023). A Survey on Secure Trust based Routing in WSN. *International Journal on Emerging Technologies, 14*(1): 36–41.