International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Trust-Based Intrusion Detection Systems in WSN: Challenges and Future Directions

Navjot Kaur, Dr. Jimmy Singla

Department of CSE, CT University, Ludhiana
navkaurtoor@gmail.com, drjimmy18086@ctuniversity.in

ABSTRACT—

In recent years, the landscape of Wireless Sensor Network (WSN) based applications ranging from military surveillance to health-related applications has grown to a giant scale due to their low cost, self-organizing capability, high sensing capability, and fault tolerance. Regardless of these advantages, WSNs is becoming vulnerable to various types of attacks due to the constrained resources of sensors, unprotected wireless communication, and open deployment of sensor nodes. Despite being protected with prevention-based security mechanisms such as encryption and authentication, the WSN still needs to be protected against many types of internal attacks. Internal attacks are harder to protect against than external ones. Recently, researchers have gained incredible interest in trust-based IDS to embed security in WSNs by defending against internal attacks. Keeping this in mind, we present a pervasive review of Trust-based IDS proposed in WSN so far to highlight their shortfalls along with the future directions in designing a lightweight and energy-aware trust-based IDS.

Index Terms—Wireless Sensor Network Security, Attacks, Intrusion Detection System, Trust mechanism.

I. INTRODUCTION

A wireless sensor network (WSN) is a distributed, self-governing network that encompasses a set of geographically dispersed autonomous sensor nodes [1]. These sensor nodes are lightweight, low-cost devices that are deployed in a specific environment [2]. Sensor nodes are independent self-configurable, capable of constructing the routing subsystem without any preexisting infrastructure, and able to work together with applications in data detection, data collection, and forward sensed data to the base station node [3]. Wireless Sensor Networks (WSNs) have grown a wide range of applications such as target tracking, military surveillance, traffic monitoring, transportation, forest fire observing, health care systems, agriculture, smart buildings, and satellite communications [4–8]. A key attraction feature of wireless sensor networks is their ease of installation and operation. However, Wireless sensor nodes are deployed in open and harsh environments with limited bandwidth and form a highly dynamic network topology, that is, a network with no predetermined architecture and no centralized network administration [9]. In WSN, all nodes collaborate with themselves to monitor the network, and each node's sensing and communication range is limited. So, they have little alternative except to collaborate with other nodes in the network [10]. Despite their impressive capabilities and wide range of applications, the security of WSNs is still a challenging task [11]. Wireless sensor networks (WSNs) are susceptible to various kinds of security attacks at all layers, less reliable, and failure-prone due to open deployment of the nodes and wireless communication between them [12]. Moreover, due to limited computational power, energy, less storage memory and low bandwidth of sensor nodes traditional energy-consuming defense mechanisms like public key infrastructure, authentication, encryption, and host-based intrusion detection techniques may not be feasible [13]. These Prevention methods usually act as the first line of defense and can protect at some level [14]. These security mechanisms are effective only against external attacks but cannot adequately defend against network insider attacks such as compromised attacks as well as routing attacks [15]. Once the node is compromised, it can potentially steal sensitive information and use it for malicious reasons such as controlling the whole WSN to degrade its performance [16]. These challenges create a lot of opportunities to take advantage of network flaws. As a result, we can't rely solely on intrusion prevention systems [17]. However, security is one of the key challenges in building a robust and reliable wireless sensor network [18]. As a second line of protection, a robust security mechanism known as Intrusion Detection Systems (IDS) is required to defend WSNs from external as well as internal attacks [19]. In recent years, trust-based intrusion detection system has emerged as an important methodology for the provision of security in wireless sensor networks. It focuses on the detection of untrusty or compromised sensor nodes and tries to isolate them from the network [20]. The concept of trust is crucial in a situation with some degree of uncertainty. In WSN, the sensor nodes are always at risk of being compromised by an external entity. In such cases, once a node is compromised it causes other SNs to misbehave and faces one of the key challenges to building a robust and reliable sensor network [21]. To preserve confidentiality, we need to ensure that the sensed data is safeguarded, all sensor nodes communicating in unattended environments are trusted, and establish secure communication. This emphasizes the importance of establishing trust between two communicating sensor nodes [22].

Nowadays, existing traditional trust mechanisms designed for the wired network as well as for wireless ad-hoc networks, are no longer suitable for WSNs due to higher resource consumption, such as memory and power [23]. In this paper, we discuss and present the fundamentals of the Trust mechanism, and the need for trust and review various existing trust-based intrusion detection systems for WSN. The review also includes various trust metrics and parameters. We also stated some of the issues in the trust-based intrusion detection systems and open research challenges.

II. TRUST-BASED INTRUSION DETECTION SYSTEM

In WSN, various strategies are used to prevent malicious nodes from interfering with the working of the network. All of the nodes are constantly in danger of being compromised by an adversary. Developing a secure network among the sensor nodes is very challenging due to the constraints of the WSN. Trust is a useful strategy for enhancing wireless network security in such a restricted and unattended environment. Malicious node identification, secure routing, secure cluster head selection, secure data collection, and intrusion detection are some of the common applications of trust in WSNs. Trust-based intrusion detection system has attracted a lot of attention among all these applications because of their flexibility against uncertainty and robustness against threats.

A. Trust: Concept and Classification

“A combined characteristic model in WSN for ensuring reliability, security, and privacy concerning mobility is called Trust,” according to one other definition of trust in WSNs [24]. Trust may be categorized in different ways based on how they are used [25-26].

- Depending on the task, trust may be subjective or objective
- Depending on the property, a trust may be a social trust or QoS trust.
- Depending on the context, the trust might be categorized as a behavioral trust or computational trust.
- Depending on stored information about the trust, it may be classified as centralized, distributed, or hybrid trust.
- Depending on the observation, a trust may be direct trust, indirect trust, or mutual trust.
- Depending upon the trust value calculation, it may be communication trust and data trust.
- Depending upon the evaluation method, trust may be hard trust or soft trust.

B. Trust Mechanism

Trust estimate methods are used in the trust mechanism for the survival of wireless sensor nodes to evaluate the dependability, reliability, and trustworthiness of sensor nodes by monitoring their actions [27]. In the WSN, the terms ”trust,” ”reputation,” and ”security” are frequently used to describe trust mechanisms where Reputation is defined as one sensor node’s perspective about the other sensor nodes and trust is defined as a level of confidence about other neighbor nodes based on their interactions. Both trust and reputation are used to make effective selections when choosing relay nodes, as well as analyzing sensed data from neighbor nodes to identify it as trustworthy or malicious [28].

C. Need of Trust Mechanisms

1) Trust provides a solution for granting corresponding access control by analyzing the behavior of sensor nodes to resolve the limitation of traditional security mechanisms.

2) Trust solves the difficulty of providing trustworthy routing paths free of any malfunctioning, selfish, or faulty nodes.

3) Trust assists network nodes in making decisions based on trust values or trust metrics.

4) By guaranteeing that all communicating nodes are trusted during authentication, authorization, or key management, trust makes traditional security services more robust and trustworthy.

D. Security threats in WSN

Security issues in WSN is larger as compared to other type of networks, such as wired network or wireless LAN due to their deployment environments and resource constraints [29]. In WSN, there are numerous well-known and a few lesser-known security attacks [30]. External attacks and internal attacks are two categories of attacks against WSNs. In an external attack, the attacker node is not a legitimate sensor network participant and uses different means of attack to reach the network [31]. A compromised node that was once a member of the network is referred to as an internal intruder. Compromised nodes actively try to disrupt or paralyze the network and are harder to detect [32]. It is the most serious issue in a sensor network, which leads to internal attacks. When an unauthorized attacker affects the operations of the network by monitoring, listen, and modifying the data stream in the communication channel is known as an internal attack [33]. The typical internal attacks in WSNs are investigated and presented as follows: denial of service attack (DoS attack), bad-mouthing attack, slander attack, on-off attack, garnished attack, reputation time-varying attack, sleeper attack, conflicting behavior attack, Sybil attack, node replication attack, selfish attack, flooding attack, selective forwarding attack, black hole attack, ballot stuffing attack, collusion attack, sinkhole attack, data forgery attack, etc. [34– 37]. According to [38] internal attackers use two types of misbehaving nodes:

• Selfish nodes: A selfish node may not intend to harm the system directly. It uses network resources but does not cooperate with other nodes and conserves battery life for its communications. A captured node could potentially be reprogrammed by an attacker to operate selfishly.

• Malicious nodes: A malicious node intends to cause the most damage to the system by producing network DoS through partitioning while saving battery life is not a priority.

III. LITERATURE REVIEW

In WSN, research work on Intrusion detection systems using the trust concept has attracted a lot of attention because it is an effective method for the detection of malicious or selfish nodes. However, we will discuss the existing approaches of trust-based IDS in detail from 2007-2020. Trust-based intrusion detection systems based on the weighting method, agent-based method, fuzzy theory, probability theory, multi-agent-based and statistics, etc. have received considerable attention from researchers and aim to improve the intrusion detection rate, resource efficiency, scalability, and robustness of WSN.

In [39-47] authors used a weighted method to calculate trust estimation. Shaikh et al. [39] presented the Group-Based Trust Management Scheme (GTMS) which provided a single trust value for the whole group. The trust value was estimated based on both direct and indirect observations Direct observations revealed successful and failed interactions, whereas indirect observations indicated the suggestions of trusted nodes for particular nodes. If the number of failed interactions grew, the transmitting node lowered the surrounding node’s trust value and viewed it as a malicious node. GTMS lowered the computational and communication costs associated with trust evaluation. However, it depended on a broadcast-based approach to gather a large number of feedback, which required more resources and energy at a different level of communication. Zhang et al. [40] proposed a novel hierarchical trust management method that reduces communication and storage costs. The author used the same hierarchical trust architecture as Shaikh et al. [39], but they took into account multi-attribute trust values instead of only one. In trust calculation, the scheme incorporates a time window and a decay function to capture the changing nature of trust. However, their approach is purely theoretical, with no consideration of what trust characteristics should be employed, how trust should be collected reliably, or how trust characteristics should be weighted to generate trust. Ishmanov et al. [41] introduced “A secure trust establishment technique for wireless sensor networks” to identify and prevent a well-known harmful internal attack: an on-off attack by incorporating a misbehavior component along with current node status. The results of the evaluations and theoretical analysis show that it is capable of detecting both persistent malicious behavior and on-off attacks. The author claims that it is useful for on-off attack mitigation, but a robust on-off TMS is impossible to construct without including the misbehavior frequency component. Various attacks like collusion attacks, blackhole attacks, and so on aren’t taken into account, which makes it impractical because collusion attacks have the potential to destroy the entire WSN. Ishmanov et al. [42] proposed a lightweight and robust trust establishment scheme for wireless sensor networks known as TMS” to mitigate different internal attacks like on-off with high detection rates by incorporating a major component misbehavior frequency. According to the author, TMS may be subject to on-off attacks, in which nodes alter their behavior regularly to harm the WSN. The main disadvantage of this trust model is its vulnerability to false positive alarms and the fact that it is only applicable to on-off attacks, which limits its use to certain situations because in reality collusion attack might affect the performance of the entire WSN. Sajjad et al. [43] proposed “Neighbor node trust-based Intrusion Detection for Wireless Sensor Networks” based on the trust computation of the neighboring node. Each node in the proposed IDS monitors the trust level of its neighbors. Neighboring nodes can be classified as trustworthy, risky, or malicious based on these trust values. Trustworthy nodes are recommended to the forwarding engine for packet forwarding purposes. By evaluating network statistics and malicious node activity, the proposed technique successfully identifies Hello flood attacks, jamming attacks, and selective forwarding attacks. Wang et al. [44], the trust for wireless sensor networks (WSNs) at the physical layer is calculated using a physical layer trust-based intrusion detection system (PL-IDS).In this direct trust value is computed as per the deviation of energy consumption (Ecm) and number of message transmissions (Nmt) at the physical layer. If the trust value falls below a certain level, the node is labeled as a malicious node. From the results, we can infer that the detection accuracy falls as the percentage of periodic jamming attackers rises. It’s also been noticed that as the network’s density rises, the detection accuracy also rises. The false alarm rate rises as the percentage of periodic jamming attackers rises, and as the network density rises, the false alarm rate drops as the data becomes denser. Singh et al. [45] propose a “Light Weight Trust mechanism (LWTM) and overhead analysis for clustered WSN.” This cluster-based WSN consists of numerous clusters with a CH and several CMs. Trust relationships between CMs (direct trust) as well as trust relationships between CH and CMs (indirect trust) are calculated. This trust model can successfully identify malicious or compromised nodes between dealing nodes, as well as identify false positive and false negative alerts, making it resistant to various attacks but there was a lack of response speed to attacks. Ghugar et al. [46] proposed a protocol layer trust-based intrusion detection system for securing the WSN by detecting attackers at different layers. The trust value of a sensor node is computed separately at the physical layer, MAC layer, and network layer using the deviation of trust metrics from the monitored node’s direct experience as well as the experiences of its neighbors. Ghugar et al. [47] designed “ML-IDS: MAC Layer Trust-Based Intrusion Detection System for Wireless Sensor Networks” based on the weighting method concept to detect back-off manipulation attacks at the MAC layer. Back-off time and successful message transmission are two MAC-layer parameters used to calculate the trust of the monitored node. The deviation parameter of a monitored node is calculated from the direct and indirect trust. In ML-IDS, when node density rises, detection accuracy (DA) rises and the false alarm rate (FAR) falls and performs better than wang et al. [44].

In [48-51] authors used the probability distribution method to determine the degree of trust of a sensor node. Liu et al. [48] author proposed a localized for insider attacker identification for wireless sensor networks, based on the spatial correlation seen in neighborhood activity. According to the authors, each node may keep track of the networking behavior of immediate neighbor nodes and evaluate them based on metrics such as packet dropping, packet sending, forwarding delay time, and sensor readings using a trust-based node assessment system. Then, if a neighbor’s conduct is ”extreme” in comparison to that of others in the neighborhood, the neighbor is accused of being an internal opponent. The experiments were conducted completely on synthetic data with a multivariate normal distribution. Li et al. [49] proposed a distributed group-based intrusion detection scheme and claim that it satisfies the characteristics of an efficient, lightweight, and flexible intrusion detection scheme by dividing sensor networks into numerous groups, each of which has sensors that are physically adjacent to one another and have the same sensing capabilities. The experiments were carried out using real data including simple sensor readings. According to the results, this scheme performs better than Liu et al. [49] in terms of two key performance metrics of intrusion detection systems i.e., false alarm ratio and detection accuracy while lowering the power consumption. Unfortunately, the authors of [48,49] do not specify any conditions in which the assumption (about multivariate normal distribution) remains true. Bao et al. [50] proposed “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection”. The technique takes into account the impact of social and QoS trust on trustworthiness and maliciousness. A probabilistic model based on stochastic Petri nets (SPN) (CH) was developed to describe the behaviors of each SN or cluster head (CH). In the peer-to-peer trust evaluation process, three different trust components as considered, namely, honesty, energy, and cooperativeness. Each SN evaluates other SNs in the same cluster while each CH other CHs and SNs in its cluster are based on these three components for trust evaluation and intrusion detection. Then a statistical method to infer the false alarm probabilities of the trust-based IDS for the minimum trust threshold. The author also presents an optimal trust threshold for minimizing false positives and false negatives and this threshold drops as the network lifespan rises. Fang et al. [51] author proposed a Beta-based Trust and Reputation Evaluation System (BTRES) for WSNs’ node trust and reputation evaluation. BTRES is based on monitoring nodes’ behavior and the beta distribution is used to characterize the distribution of nodes’ reputation, and then calculate the trust value. By setting weight and threshold values, collusion attacks on compromised nodes can be effectively countered. The trust value of nodes can be used in routing protocols or aggregation mechanisms. The proposed approach can maintain network security by prioritizing the node with the highest trust value while choosing a routing path or aggregating data.

In [52-54] fuzzy theory method is used for the calculation of trust. Wu et al. [52] proposed a trust model based on fuzzy theory and evidence theory for detecting anomaly nodes in WSNs. The detection rate of this proposed model is better than the model proposed by Shaikh et al. [39]. Feng et al. [53] proposed “A trust evaluation algorithm for wireless sensor networks based on node behavior and d-s evidence theory” known as NBBTE. To identify malicious nodes, the NBBTE method initially develops various trust factors based on neighbor node interactions that are witnessed by each other. The trust value is calculated by integrating network security degree and correlation of time context. Then, it uses fuzzy set theory to determine how much each trust degree’s trust value belongs to each node. Finally, the integrated trust value of evaluation incorporating the recommendations of several neighbor nodes is obtained using the trust difference between evidence and the improved Dempster rule of combination. Subjectivity, uncertainty, and fuzziness of trust evaluation are all taken into consideration by the proposed model when analyzing nodes’ trustworthiness. Higher communication and memory overhead make the NBBTE model non-realistic for large-scale WSNs. Shao et al. [54] suggested a lightweight and dependable trust model for clustered WSNs, in which the fuzzy degree of nearness is used to assess the trustworthiness of suggested trust values from third-party nodes to calculate a sensor node’s trust degree. The proposed scheme outperforms shaikh et al. [39]

In [55-56] some miscellaneous methodology was used by authors to evaluate the trustworthiness of the node. Sedjemalci et al. [55] developed an “Efficient and Lightweight Intrusion Detection System based on Nodes’ Behaviors in Wireless Sensor Networks (ELID)” to detect the most dangerous routing attacks such as Selective forwarding, Sinkhole attacks Blackhole Attacks, Warmhole Attacks, and Denial of service (DoS). The author proposed two types of agents Intrusion Detection Agent (IDA) and Decision-Making Agent (DMA) for intrusion detection and decision purpose. This detection policy is based on the concept that all the nodes that are located within the same cluster should have similar behaviors. IDA applies a behavior-based detection to detect malicious nodes and this agent is activated at cluster member level. DMA activates at cluster head level. It checks whether the suspected node detected by IDA is malicious or not. Then it mitigates the number of false positives in its decision-making module. Both agents work in a collaborative mode to detect malicious nodes with high accuracy. Results show that ELID exhibits a high detection rate, low false positive rate, very low energy consumption, and requires less time to detect routing attacks. ELID performs better than Shaikh et al. [39] in terms of attack detection and energy consumption. Jin et al. [56] proposed a Mutli-agent trust-based intrusion detection system for layer cluster WSNs. In this multi-agent model, agents collaborate to calculate trust values. Mahalanobis distance is used to judge node trust feature abnormalities to make judgments more accurate and to improve trust value accuracy. A combination of a tolerance factor and beta distribution was introduced to calculate and update trust values. This scheme enhances the system's fault tolerance and has a high detection performance.

TABLE I SUMMARY OF THE EXISTING TRUST-BASED IDSS FOR WSN

Research Paper	**Methodology**	**Performance Metrics**	**Attacks detected**	**Limitations**
Liu et al. [48]	probability theory detection	accuracy, false alarm	malicious insider attackers	Results represent a tradeoff between communication overhead and performance.
Li et al. [40]	probability theory detection	accuracy, false alarm	malicious insider attackers	it usually focuses on the trust values of individual nodes and the trust evaluation cost is high
Shaikh et al. [39]	weighted method	communication overhead, energy consumption	bad-mouthing, node replication, selective forwarding, and sinkhole attack	it is attack-resistant under an assumption i.e. not always true. This makes it not suitable for real-time application

Feng et al. [51]	fuzzy theory	communication overhead, energy consumption	on-off attack	higher memory and energy requirement, non-realistic for large WSN
Ishmanov et al. [42]	binomial method	false-positive rate, false-negative rates	on-off attack	model is sensitive to false positive alarms and only specific to on-off attack
Sajjad et al. [43]	weight method	detection rate	Hello flood, jamming and selective forwarding attack	it does not consider risky attacks
wang et al. [44]	binomial method	trust threshold, energy consumption, idle time, number of retransmission route metric, packet forwarding rate	back-off manipulation, selective forwarding, sinkhole attack, cross-layer attack	communication overhead increases with the increasing of the hop count to cluster head

IV. TRUST METRICES

Trust metric is a measure of how others perceive a member of one group. The trust model uses numerous trust metrics to determine the trust value for the node. It may be classified as deterministic or probabilistic, binary, discrete or continuous, and symmetric or asymmetric. From the literature discussed above, it is observed that selecting proper trust metrics to calculate the trustworthiness of an SN is essential. There are no universal criteria for the selection of the trust factor to calculate trust metrics. Some of the trust metrics or parameters are as follows:

1) Energy consumption: The amount of energy used by a node to compute trust for its neighbors and to exchange that trust with them.

2) Trust update interval: time duration after which the confidence of a node is gained about that node from its neighbor node's perspective.

3) Hop count: The number of nodes that a packet passes through on its way from its source to its destination.

4) Transmission radius: The range within which a node might send packets to other nodes.

5) Packet forwarding rate: The number of packets a node receives from its neighbors and then forwards to its parent node over a certain period.

6) Idle time: The time duration between two consecutive successful transmissions of malicious nodes 7) Number of retransmissions: Total number of times after a node successfully transmits data.

8) False acceptance rate: It is the measure of a false positive that occurs when a node believes its neighbor is malicious when it is not.

9) Missed detection rate: It is the measure of a false negative that occurs when a node fails to identify a malicious node in its immediate vicinity.

10) Trust level: Level of the confidence of a node about its neighbor node.

V. OPEN RESEARCH CHALLENGES

We have discussed so far various existing Trust-based IDS in WSN. Furthermore, based on the literature review we summarized them based on different criteria like methodology, trust metrics, attacks detected, etc. as shown in above Table 1. We observed that there are still various issues that remain to be addressed. In this section, we will highlight them and list them below:

- The major disadvantage of fuzzy-based anomaly detection is that it depends on the rules of the fuzzy inference engine and cannot handle anomalies that are not covered by rules, resulting in a significant number of false negatives when unknown anomalies emerge.

- A significant issue with anomaly detection is a high rate of false alarms, which can be caused by noise in wireless transmission, as well as a lack of resources to collect relevant and essential data.

- Probability-based IDS have computational complexity and also require high energy which is not feasible for resource-constrained WSN. When trust is simulated using weighted approaches, the granularity of the trust connections may be poor.

- For the aforementioned trust mechanisms, there are hardly any thorough simulations available. In reality, the majority of the papers lack extensive analysis or simulations.

- Although many Trust-based IDS have been proposed to detect malicious or selfish nodes, most of them are attack-specific and target only one or two attacks and also one or two network layers.

- Energy efficiency, memory requirement, computation complexity, and communication overhead are the main design considerations for WSN-based applications. But in the case of existing approaches, there is always a trade-off between these parameters and it will unavoidably have an impact on the network's lifespan.

- It has been found that choosing appropriate trust measures to calculate an SN's trust is quite important because it has a significant impact on the performance of the detection algorithm.

- Very little work has been done on IDS for mobile sensor nodes in WSNs.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this review, we have provided a detailed and comprehensive study of existing trust-based intrusion detection systems in wireless sensor networks. We have started with the term "trust" and classifying it based on how they are used. In addition, we have introduced a trust mechanism and its need in WSN. Next, we have briefly introduced several existing internal attacks in WSN. Furthermore, we have provided a literature review of existing trust-based IDS in WSN based on different methodologies. Based on our observation and findings, we have provided some trust metrics or trust factors found in the existing trust-based IDS. In the end, we can conclude that there are still various issues associated with the existing IDS that need to be further solved. To address these issues in the future, additional work has to be done on IDS that are lightweight for resource-constrained WSNs and consume the least amount of energy. To give optimum detection accuracy, it should also be a cross-layer IDS that can identify both known and unknown attacks.

REFERENCES

[1] M. Aboelaze and F. Aloul, "Current and future trends in sensor networks: a survey," in Second IFIP International Conference on Wireless and Optical Communications Networks, 2005. WOCN 2005. IEEE, 2005, pp. 551–555.

[2] M. Tubaishat and S. Madria, "Sensor networks: an overview," IEEE Potentials, vol. 22, no. 2, pp. 20–23, 2003.

[3] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," IEEE Communications surveys & tutorials, vol. 11, no. 2, pp. 52–73, 2009.

[4] L. M. Borges, F. J. Velez, and A. S. Lebres, "Survey on the characterization and classification of wireless sensor network applications," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1860–1890, 2014.

[5] Đurišić, M. P., Tafa, Z., Dimić, G., & Milutinović, V. (2012, June). A survey of military applications of wireless sensor networks. In *2012 Mediterranean conference on embedded computing (MECO)* (pp. 196-199). IEEE.

[6] García-Hernández, C. F., Ibarguengoytia-Gonzalez, P. H., García-Hernández, J., & Pérez-Díaz, J. A. (2007). Wireless sensor networks and applications: a survey. *IJCSNS International Journal of Computer Science and Network Security*, *7*(3), 264-273.

[7] K. F. Navarro and E. Lawrence, "Wsn applications in personal healthcare monitoring systems: a heterogeneous framework," in 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine. IEEE, 2010, pp. 77–83.

[8] H. M. A. Fahmy, "Wsn applications," in Concepts, Applications, Experimentation and Analysis of Wireless Sensor Networks. Springer, 2021, pp. 67–232.

[9] S. Srivastava, M. Singh, and S. Gupta, "Wireless sensor network: a survey," in 2018 International Conference on Automation and Computational Engineering (ICACE). IEEE, 2018, pp. 159–163.

[10] G. J. Pottie, "Wireless sensor networks," in 1998 Information Theory Workshop (Cat. No. 98EX131). IEEE, 1998, pp. 139–140.

[11] A. Rani and S. Kumar, "A survey of security in wireless sensor networks," in 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT). IEEE, 2017, pp. 1–5.

[12] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," 2006. [13] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks," Journal of sensors, vol. 2015, 2015.

[14] D. G. Padmavathi, M. Shanmugapriya et al., "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv:0909.0576, 2009.

[15] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013.

[16] D. Martins and H. Guyennet, "Wireless sensor network attacks and security mechanisms: A short survey," in 2010 13th International Conference on Network-Based Information Systems. IEEE, 2010, pp. 313–320.

[17] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," Information Security Technical Report, vol. 10, no. 3, pp. 134–139, 2005.

[18] A. H. Farooqi and F. A. Khan, “Intrusion detection systems for wireless sensor networks: A survey,” in International Conference on Future Generation Communication and Networking. Springer, 2009, pp. 234– 241.

[19] K. Kaur and N. Kaur, “A hybrid approach of fuzzy c-mean clustering and genetic algorithm (ga) to improve intrusion detection rate,” International Journal of Science and Research, 2015.

[20] Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures,” Journal of Network and computer Applications, vol. 35, no. 3, pp. 867–880, 2012.

[21] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, “Trust management systems for wireless sensor networks: Best practices,” Computer Communications, vol. 33, no. 9, pp. 1086–1093, 2010.

[22] X. Li, F. Zhou, and J. Du, “Ldts: A lightweight and dependable trust system for clustered wireless sensor networks,” IEEE transactions on information forensics and security, vol. 8, no. 6, pp. 924–935, 2013.

[23] N. Kaur and P. Rattan, “A critical review of intrusion detection systems in wsn: Challenges & future directions,” Annals of the Romanian Society for Cell Biology, pp. 3020–3028, 2021.

[24] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, “Trust management in wireless sensor networks,” European Transactions on Telecommunications, vol. 21, no. 4, pp. 386–395, 2010.

[25] V. U. Rani and K. S. Sundaram, “Review of trust models in wireless sensor networks,” Int. J. Comput. Inf. Syst. Control Eng, vol. 8, pp. 371–377, 2014.

[26] W. Luo, W. Ma, and Q. Gao, “A dynamic trust management system for wireless sensor networks,” Security and Communication Networks, vol. 9, no. 7, pp. 613–621, 2016.

[27] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, “Trust management system in wireless sensor networks: design considerations and research challenges,” Transactions on Emerging Telecommunications Technologies, vol. 26, no. 2, pp. 107–130, 2015.

[28] F. Zawaideh and M. Salamah, “An efficient weighted trust-based malicious node detection scheme for wireless sensor networks,” International Journal of Communication Systems, vol. 32, no. 3, p. e3878, 2019.

[29] K. Chelli, “Security issues in wireless sensor networks: Attacks and countermeasures,” in Proceedings of the World Congress on engineering, vol. 1, no. 20, 2015, pp. 876–3423.

[30] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor network security: a survey,” IEEE Communications surveys & tutorials, vol. 11, no. 2, pp. 52–73, 2009.

[31] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE communications surveys & tutorials, vol. 16, no. 1, pp. 266–282, 2013.

[32] Z.-T. Lin, Y.-G. Qu, L. Jing, and B.-H. Zhao, “Compromised nodes in wireless sensor network,” in Asia-Pacific Web Conference. Springer, 2006, pp. 224–230.

[33] M. R. Ahmed, X. Huang, and D. Sharma, “A taxonomy of internal attacks in wireless sensor network,” Memory (Kbytes), vol. 128, p. 48, 2012.

[34] Y. A. Bangash, Y. E. Al-Salhi, et al., “Security issues and challenges in wireless sensor networks: A survey.” IAENG International Journal of Computer Science, vol. 44, no. 2, 2017.

[35] J. Sen, “A survey on wireless sensor network security,” arXiv preprint arXiv:1011.1529, 2010.

[36] M. Z. A. Bhuiyan and J. Wu, “Collusion attack detection in networked systems,” in 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). IEEE, 2016, pp. 286–293.

[37] S. Sharma, R. K. Bansal, and S. Bansal, “Issues and challenges in wireless sensor networks,” in 2013 International Conference on Machine Intelligence and Research Advancement. IEEE, 2013, pp. 58–62.

[38] O. Khalid, S. U. Khan, S. A. Madani, K. Hayat, M. I. Khan, N. MinAllah, J. Kolodziej, L. Wang, S. Zeadally, and D. Chen, “Comparative study of trust and reputation systems for wireless sensor networks,” Security and Communication Networks, vol. 6, no. 6, pp. 669–688, 2013.

[39] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Lee, S. Lee, and Y.-J. Song, “Group-based trust management scheme for clustered wireless sensor networks,” IEEE transactions on parallel and distributed systems, vol. 20, no. 11, pp. 1698–1712, 2008.

[40] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, and A. Sattar, “A dynamic trust establishment and management framework for wireless sensor networks,” in 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. IEEE, 2010, pp. 484–491.

[41] F. Ishmanov, S. W. Kim, and S. Y. Nam, “A secure trust establishment scheme for wireless sensor networks,” Sensors, vol. 14, no. 1, pp. 1877–1897, 2014.

[42] Ishmanov, F., Kim, S. W., & Nam, S. Y. (2015). A robust trust establishment scheme for wireless sensor networks. *Sensors*, *15*(3), 7040-7061.

[43] S. M. Sajjad, S. H. Bouk, and M. Yousaf, “Neighbor node trust-based intrusion detection system for wsn,” Procedia Computer Science, vol. 63, pp. 183–188, 2015.

[44] J. Wang, S. Jiang, and A. O. Fapojuwo, “A protocol layer trust-based intrusion detection scheme for wireless sensor networks,” Sensors, vol. 17, no. 6, p. 1227, 2017.

[45] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar, “A lightweight trust mechanism and overhead analysis for clustered wsn,” IETE Journal of research, vol. 63, no. 3, pp. 297–308, 2017.

[46] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, “Lb-ids: Securing wireless sensor network using protocol layer trust-based intrusion detection system,” Journal of Computer Networks and Communications, vol. 2019, 2019.

[47] U. Ghugar and J. Pradhan, “Ml-ids: Mac layer trust-based intrusion detection system for wireless sensor networks,” in Computational Intelligence in Data Mining. Springer, 2020, pp. 427–434.

[48] F. Liu, X. Cheng, and D. Chen, “Insider attacker detection in wireless sensor networks,” in IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications. IEEE, 2007, pp. 1937– 1945.

[49] G. Li, J. He, and Y. Fu, “A group-based intrusion detection scheme in wireless sensor networks,” in 2008 The 3rd International Conference on Grid and Pervasive Computing-Workshops. IEEE, 2008, pp. 286–291.

[50] F. Bao, R. Chen, M. Chang, and J.-H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” IEEE transactions on network and service management, vol. 9, no. 2, pp. 169–183, 2012.

[51] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, “Btres: Beta-based trust and reputation evaluation system for wireless sensor networks,” Journal of Network and Computer Applications, vol. 59, pp. 88–94, 2016.

[52] R. Wu, X. Deng, R. Lu, and X. Shen, “Trust-based anomaly detection in wireless sensor networks,” in 2012 1st IEEE International Conference on Communications in China (ICCC). IEEE, 2012, pp. 203–207.

[53] R. Feng, X. Xu, X. Zhou, and J. Wan, “A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory,” Sensors, vol. 11, no. 2, pp. 1345–1360, 2011.

[54] N. Shao, Z. Zhou, and Z. Sun, “A lightweight and dependable trust model for clustered wireless sensor networks,” in International Conference on Cloud Computing and Security. Springer, 2015, pp. 157–168.

[55] H. Sedjelmaci and S. M. Senouci, “Efficient and lightweight intrusion detection based on nodes’ behaviors in wireless sensor networks,” in Global Information Infrastructure Symposium-GIIS 2013. IEEE, 2013, pp. 1–6. [56] X. Jin, J. Liang, W. Tong, L. Lu, and Z. Li, “Multi-agent trust-based intrusion detection scheme for wireless sensor networks,” Computers & Electrical Engineering, vol. 59, pp. 262–273, 2017