Review Article

Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks

Zhengxin Xia 1,2, Zhe Wei 3, and Huan Zhang 3

1 College of Continuing Education, Nanjing University of Posts and Telecommunications, Nanjing 210042, China
2 Engineering Research Center of Medicine Information, Nanjing University of Posts and Telecommunications, Nanjing 210042, China
3 School of Computer Science, Civil Aviation Flight University of China, Guanghan 618307, China

Correspondence should be addressed to Zhe Wei; findwei@foxmail.com

Received 13 July 2022; Revised 28 August 2022; Accepted 7 September 2022; Published 27 September 2022

Copyright © 2022 Zhengxin Xia et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The scale of wireless sensor networks changes depending on specific application tasks. How to design a relatively simple security mechanism that can extend with the expansion of network scale is an arduous task. As the wireless sensor network mostly adopts the decentralized organization form, once the network nodes are distributed adequately, it is difficult to find out the failure of any node. In addition, the node has weak resistance to physical damage, so any node in the network may potentially become a cause of security vulnerability. In this study, firstly, the security standards that wireless sensor networks should have and the current security challenges are discussed in detail, and the importance of security issues in wireless sensor networks is pointed out. Secondly, this paper studies and analyzes the current situation of wireless sensor network security problems including the internal and external attacks and the active and passive attacks. Thirdly, this paper also discusses the significance, concept, and characteristics of reputation and trust, the division and composition of reputation and trust system, and the common applications of the reputation and trust mechanism in wireless sensor networks.

1. Introduction

The objects processed by computer systems are mainly abstract things, and these systems do not have insight into the real physical world. Sensors are able to measure the physical quantities such as temperature, pressure, light wave, velocity, electromagnetic wave, and so on and convert the measurement results into electronic signals. Therefore, for computer systems or computeable devices, sensors build a bridge from the abstract world to the real world so that the former can obtain almost all kinds of physical information in the real world. However, different from the traditional wired networks, wireless sensor networks, or WSNs, we usually do not need centralized management or fixed infrastructure such as base station and access point. Sensor nodes form the network automatically, and the network cost is relatively low. Therefore, WSNs can be used in situations where there is no infrastructure, or for security reasons, the existing infrastructure does not meet certain conditions. Although WSNs are widely used, security and reliability should be the prerequisite for these applications.

In this study, firstly, the security standards that wireless sensor networks should have and the current security challenges are discussed in detail, and the importance of security issues in wireless sensor networks is pointed out. Besides, it is of vital importance to develop new security technologies or modify existing security technologies for wireless sensor networks because some traditional security technologies cannot run directly on the network nodes due to their relatively complex algorithms. Secondly, this paper studies and analyzes the current situation of wireless sensor network security problems including the internal and external attacks and the active and passive attacks. Thirdly, this paper also discusses the significance, concept, and
characteristics of reputation and trust, the division and composition of reputation and trust system, and the common applications of the reputation and trust mechanism in wireless sensor networks.

2. Security Standards and Challenges

In any computer-related environment, security is considered as a nonfunctional requirement, which is not only used to maintain the availability and reliability of the whole system but also related to the protection of information and system. However, in wireless sensor networks, security issues are particularly important because on the one hand, the hardware functions of network nodes are seriously limited, and it is necessary to provide sufficient protection to protect them from malicious attacks; on the other hand, the deployment environment of wireless sensor networks makes it easy for the enemy to obtain sensor nodes illegally and destroy them [1–4]. Any destruction and interference to nodes will have a certain impact on the information obtained in the real world. It is due to the above reasons that WSNs security objectives should have the following standards [5–8], which is shown in Figure 1.

Confidentiality. Confidentiality generally refers to that unauthorized users cannot obtain confidential or sensitive information, such as network routing information, topology information, and node geographic location information. In wireless sensor networks, confidentiality provides a basic security service for the important data transmitted between network nodes. Confidentiality also ensures that the nodes cannot be eavesdropped or tampered by the third party during data transmission. In the specific implementation process, confidentiality is generally achieved by the secret key mechanism; that is, data packets are encrypted at the sender and decrypted at the receiver. Without the relevant secret key, it is difficult for attackers to access the encrypted information. In addition, it should be pointed out that the data transmitted between nodes does not need to be encrypted. For example, only the data part in the packet is encrypted during data transmission, while in other applications, only the header of the packet is encrypted to protect the identity information of nodes.

Availability. Availability ensures that network services exist for authorized users; that is, when authorized users need to use some network services, these services exist and are available. In wireless sensor networks, on the one hand, data availability ensures that all nodes submit data to the base station on time, and whenever necessary, the whole network can provide relevant services. In addition, the availability also ensures that nodes are safe and available in the presence of certain attacks.

Integrity. Integrity makes the data in the whole path between the sender and the receiver without being changed by the enemy [9]. In wireless sensor networks, the integrity of data is particularly important because the nodes are often exposed and unattended, and the communication channel between nodes is also open. Therefore, the transmitted data are easy to be interfered by the enemy channel making the integrity of the data changed.

Authentication. Authentication enables one party to ensure the legal identity of the other party with whom to communicate, that is, to ensure that the other party is not illegal or fake. In wireless sensor networks, authentication makes the sensing data obtained by the network to come from reliable information sources, and authentication also ensures the reliable identity of communication nodes in the network. In the actual operation of the network, each node should check whether the data it receives come from the real sender.

Data Freshness. Data freshness ensures that the sensing data sent by nodes in wireless sensor networks is up to date rather than out of date. Data freshness also ensures that the data sent by nodes to base stations can reflect the current situation. At the same time, data freshness can also be used to prevent malicious nodes from sending outdated and invalid information [10].

Forward and Backward Secrecy. Because nodes in the wireless sensor network have certain constraints on energy supply, some nodes will quit the network due to energy exhaustion after working for a certain period of time. At the same time, according to different application scenarios, there might be new nodes in the network. Therefore, it is necessary to prevent the exiting nodes from breaking the confidentiality of the network, and similarly, it is also necessary to prevent nodes that have just joined the network from cracking any previously used confidential information [11].

Access Control and Nonrepudiation. Only authorized users can access and use the resources and services provided by the network. Generally, the network should specify the member’s permission or the permission group to which the member belongs in advance. Nonrepudiation means that the receiving node cannot deny the data packets it has received, and the sending node cannot deny the data packets it has sent.

The scale of wireless sensor networks will change depending on specific application tasks. How to design a relatively simple security mechanism that can extend with the expansion of network scale is an arduous task. In most cases, it is necessary to find a compromise between the network performance and the security mechanism. As the wireless sensor network mostly adopts the decentralized organization form, once the network nodes are distributed adequately, it is difficult to monitor the actual working state of each node, and it is difficult to find out the failure of any node. In addition, the node has weak resistance to physical damage, so any node in the network may potentially become a cause of security vulnerability.
3. Internal/External and Passive/Active Attacks

In wireless sensor networks, due to the deployment environment and the limited hardware structure, sensor nodes are more vulnerable to the attacks. Wireless sensor network attacks can be divided into external attacks and internal attacks, and internal attacks are the main security risks of the network. This is because the malicious behavior of nodes in the network or network attacks launched by malicious nodes often disturbs and destroys the normal working nodes in the network. If these attacks are not prevented and handled, they will bring great harm to the whole network. In addition, network attacks can be further divided into active attacks and passive attacks, and active attacks are more harmful in ad hoc wireless sensor networks [12]. WSN attacks are shown in Figure 2.

3.1. Internal Attacks and External Attacks. In wireless sensor networks, all nodes are cooperative entities. External attackers are isolated from the network and have no access to the network. Generally, the impact of attacks launched by external attackers on the network is limited, but once the attacker captures the internal nodes of the network and destroys them, such as programming the captured nodes again to execute malicious programs or using nodes with more computing and storage capabilities to replace the captured nodes, the attacks become internal attacks. In contrast, the internal attack is more destructive to the network because the internal nodes are often regarded as legitimate nodes. Internal attacks are more difficult to detect and prevent; for example, the captured nodes can steal confidential information from encrypted data, transfer false information, and modify routing data.

3.2. Passive Attacks and Active Attacks. In passive attacks, the attacker’s purpose is to eavesdrop on the flowing information in the network without being detected by the system. Through passive participation in network internal activities, attackers can also obtain a large number of data and conduct data analysis to extract key information. However, due to the lack of clues left by passive attackers, it is difficult to be found.

In active attacks, the attacker can make use of the security loopholes in the network protocol to launch a variety of attacks, such as modifying and deleting the data packets in the routing to make the routing protocol unreliable; for example, in the replay attack, the attacker will maliciously resend the valid routing data packets sent before. The direct result is that the data packets are sent to the wrong destination or make invalid loops in the network, which will eventually lead to network congestion.

Further, a successful active attack by an attacker will seriously damage the function of the network and cause the system to make a wrong judgment and decision. In addition,
4. Trust Mechanism

4.1. Concept and Definition. In social science, trust can be understood as follows [16–19]: in social networks, trust refers to the behavior that one party voluntarily relies on the other party in a special environment; trust can also be understood as an intention, i.e., one party intentionally relies on the other party.

In the field of computer science, for example, in a routing information request task, the former is the trustor and the latter is the trusted party. When the routing information is successfully transmitted, it is considered to be a node with good behavior, and then its trust value will be increased; on the contrary, when providing wrong routing information, a node is considered as a malicious node, and the corresponding reduced reputation value is applied as a punishment method. In this mechanism, trust is undoubtedly a double-edged sword. On the one hand, it will consume some resources of the system, and on the other hand, it will greatly improve the security of the system.

4.2. Division and Composition of Trust. According to the storage and access of reputation information, the reputation and trust system can be divided into centralized system and decentralized/distributed system. Large e-commerce websites such as Amazon mostly adopt the centralized reputation system and store reputation data in the database associated with websites [20]. For wireless sensor networks, although the centralized reputation system has certain advantages, due to the special structure of network and network nodes, the network system often adopts the decentralized reputation system. In wireless sensor networks, the reputation and trust mechanism has the following characteristics:

1. The mechanism of reputation and trust provides incentives for the benign development of node behavior; that is, it makes nodes more responsible for their own behavior.
2. The reputation and trust mechanism provides the prediction of the future behavior of nodes, which can assist in decision-making.
3. The reputation and trust mechanism makes the nodes with good behavior avoid cooperating with the nodes that lack trust. The malicious behavior of nodes leads to the low reputation of nodes themselves, which also makes such nodes have no more opportunities to participate in network cooperation.
4. The reputation and trust mechanism is also conducive to the detection of selfish nodes in the network and timely isolation of malicious nodes in the network.

5. Common Applications of Trust

Reputation and trust mechanisms have been widely studied and applied in distributed systems such as ad hoc networks, P2P networks, grid computing, pervasive computing, and e-commerce. In wireless sensor networks, the reputation and trust mechanism can be combined with other network function algorithms to provide better guarantee and service for the network. Specifically, the reputation and trust mechanism can be applied to the following aspects of wireless sensor networks:

5.1. Trusted Data Fusion. In order to ensure the reliability and credibility of data fusion in wireless sensor networks, studies in Refs. [21–33] introduced the reputation mechanism into the network data fusion scheme. In order to deal with the potential malicious nodes in the process of data fusion, combined with reputation management and encryption technology, Ref. [21] proposed a trust-based security data fusion method named blind observation. By adapting the order preserved encryption technology and the sigmoid trust model, the blind observation method can distinguish malicious nodes without decrypting the data sent to the base station and checking the data inside. The security and reliability of data fusion can be ensured by this method. However, in ad hoc wireless sensor networks, the captured or attacked nodes still hold network encrypted information, which is not discussed in Ref. [21].

In order to improve the security of data fusion, Ref. [23] proposed a trust-based intranetwork data fusion method. This method uses the tree data fusion structure and a reputation model based on binomial distribution to detect malicious behavior of nodes. In Ref. [23], the reputation measurement of a node is evaluated by the data it sends, its routing behavior, and its availability. In order to achieve the purpose of reliable data fusion, network nodes only send data to the data fusion nodes whose credibility is higher than the specified threshold value for fusion operation. Although this method may provide security for data fusion, it does not discuss whether the qualified data fusion nodes can rotate to
balance the energy distribution of nodes. In addition to using the tree data fusion structure,Refs. [24, 25] also use the cluster structure. In Ref. [25], the data from the node are weighted according to the reputation of the corresponding node, and the common node selects the fusion point according to the reputation of the data fusion node.

To obtain high quality sensory data, Ref. [28] proposed an energy efficient data fusion method ETA based on the binomial reputation model. ETA adopts the cluster node topology structure and uses the reputation mechanism to select the nodes that meet the requirements as data fusion nodes. In addition, in order to find the best path from ordinary nodes to data fusion nodes, ETA also takes into account the residual energy of nodes on the path and the availability of links. In this method, each node maintains two reputation tables: the reputation table about the link availability of the neighbor node and the reputation table about the data fusion ability of the neighbor node. ETA assumes that the location of each node and base station are known in advance and that there is no malicious node injecting false data in the network. But ETA also has the following problems: each node in the cluster must send its data to the upstream node designated by the base station node, which will increase the complexity of the network; to determine the availability of the link between nodes, each node must send data to its neighbor nodes, which will bring extra cost to the network.

RDAs [22] improve the robustness of data fusion by using the reputation mechanism to identify and isolate malicious nodes in the wireless sensor network data fusion algorithm. The nodes in RDAs adopt the cluster structure and distributed-reputation mechanism. Each node keeps the reputation information of other nodes in the cluster locally and shares the reputation information with other nodes in the cluster. RDAs use LEACH as the underlying data fusion protocol and use the reputation model based on binomial distribution as the node reputation evaluation method.

To ensure the reliability and credibility of data transmitted in WSNs, Ref. [29] proposes a trust evaluation model and data fusion mechanism, which is composed of behavioral trust, data trust, and historical trust. The data trust can be obtained by processing the sensor data, and according to the sensing and forwarding behavior of nodes, the behavior trust is computed. Reference [30] proposes a data fusion and transfer learning empowered granular trust mechanism to handle the data reliability. In order to prevent privacy disclosure and task destruction, a dynamic reward and punishment mechanism is designed to encourage honest users and accurately assess user trust. Reference [31] introduces a data fusion trust model based on rational attributes. It relies on different time attributes to identify the trust of available services, and deep machine learning is used to recursively analyze the attributes and uncertainty characteristics of service providers in continuous shared instances to fuse data with less uncertainty. Reference [32] proposes a trust fusion method consistent with the consortium chain to reach consensus and complete self-organized trust decentralized collaborative learning. In this method, consensus candidates will check others’ trust level to ensure that they tend to integrate consensus with users with high trust. Reference [33] proposes a lightweight privacy protection trust evaluation scheme, which can fully balance trust evaluation and privacy protection under low cost so as to facilitate distributed data fusion.

5.2. Trusted Routing

In wireless sensor networks, all nodes are not only the sender of data sets but also the routing and transmission of data from third-party nodes. Therefore, how to route data to the destination through the reliable transmission path becomes one of the key problems in the design and operation of wireless sensor networks when some nodes in the network behave abnormally and violate the specified standards.

Most routing protocols in wireless sensor networks only consider how to maintain the path connectivity between the source node and the destination node and use methods such as the shortest path or minimum spanning tree to construct the data path. However, the above methods rarely consider whether the intermediate nodes involved in the path will cooperate with other nodes to complete the routing and transmission of data packets. Therefore, it is reasonable to think that some intermediate nodes for their own interests (such as legitimate nodes do not respond to the route to save their energy and illegal nodes tamper with data or selectively discard packets) do not complete the routing or packet delivery task according to the protocol. If the routing protocol in wireless sensor network does not have a method to identify selfish behavior or malicious behavior of nodes, the established path may contain the above two kinds of nodes. Therefore, the path may be unstable, the reliability and integrity of data transmission cannot be guaranteed, and the efficiency of the whole network is also low [34].

In order to improve the reliability and security of routing protocols in wireless sensor networks and protect the network from the influence of abnormal behaviors of nodes, the reputation system is combined with the routing protocols of wireless sensor networks in Ref. [34], and the abnormal behaviors of nodes are divided into two categories: selfish behaviors and malicious behaviors. Different processing methods are adopted according to different abnormal behaviors of nodes, the reputation mechanism based on Bayesian theory is combined into the network routing protocol, and the reliability of each node is evaluated according to the data packet delivery. Finally, the reliable data routing path is established according to the reliability of the node.

According to the observation results of data transmission behavior of nodes, Ref. [34] divides sensor nodes into three categories: friendly, selfish, and malicious. The friendly node will submit the received data packets as they are to ensure the integrity of the submitted data; selfish nodes will randomly discard all or part of the data packets due to their own physical conditions, such as lack of power supply energy, overload, and other reasons, so as to maintain their own physical conditions, and selfish nodes will undoubtedly reduce the reliability of the network; the security and integrity of the network system are often reduced by malicious
nodes modifying the contents of the received data packets or deliberately routing the data packets to the wrong receivers.

Reference [35] proposes a trust model based on node behavior to deal with malicious nodes in opportunistic routing and forwarding candidate set. By using pruning and filtering mechanisms, it deletes malicious suggestions and uses dynamic weight calculation method to combine direct trust and indirect trust to get the comprehensive trust. In order to resist attacks such as black hole and selective forwarding, Ref. [36] proposes a trust aware secure routing protocol to resist these attacks, in which each node calculates the comprehensive trust value of its neighbors based on the direct trust, the indirect trust, the volatility factor, and the residual energy. Reference [37] proposes an atomic search sunflower optimization method to provide trust based routing. The method is designed by combining sunflower optimization with atomic search optimization and uses multiple trust factors to identify and isolate attacks and optimize network performance. By using the Markov chain prediction model, Ref. [38] proposes a reliability trust evaluation model for secure routing based on the combination of internal states of nodes and external interaction between nodes. By selecting security nodes based on tolerance constants and selecting opportunity nodes from security nodes for routing, Ref. [39] proposes a routing algorithm based on energy aware trust and opportunity, which uses multipath routing technology with the multihop communication mechanism within and between clusters.

5.3. Malicious Node Detection. The security threats of wireless sensor networks come not only from external attacks but also from internal attacks of internal nodes. Although traditional security mechanisms such as the encryption mechanism and the authentication mechanism can prevent some external attacks, these security mechanisms are not so effective for attacks launched by internal nodes with abnormal behavior. Reference [40] proposed a malicious node detection mechanism based on the reputation mechanism. This method adopts the reputation model of Bayesian statistical inference and adds the indirect reputation recommendation from the third party. In Ref. [41], the behavior of malicious nodes modifying data packets was identified by every node monitoring each other. By analyzing the signal strength of data readings received by the physical layer of wireless sensor network nodes, Ref. [42] identifies and prevents malicious nodes that send noise to the network and cause channel conflict. Based on the binomial reputation model, Ref. [43] proposed a location aware method for malicious node isolation and deletion in wireless sensor networks.

In addition, in order to effectively isolate malicious nodes, Ref. [44] introduces the reputation system into the routing protocol. Its basic principle is that any node in the network uses a certain mechanism to monitor its neighbors and evaluates its trust value according to the behavior of the monitored node; when the reputation value of a neighbor node is less than the defined threshold value, the neighbor node will be considered as a suspicious node. In this algorithm, the change of trust value of neighbor nodes only depends on the observer node. Each observer node shares its suspicious node information, so the noncooperative node will be punished soon. However, this method cannot identify the cheating behavior of malicious nodes. It is only a theoretical framework, and no specific and effective reputation evaluation method is given.

To avoid being judged as a malicious node by the reputation system when the reputation value is lower than the predefined reputation threshold value, and finally isolated by the system, some malicious nodes will attack intermittently and maintain good behavior in the period of not launching the attack so as to obtain a good reputation so that their reputation is generally higher than the reputation threshold. In order to solve the above problems, Ref. [45] proposed a malicious node identification method based on node reputation and time series analysis. In this method, malicious suspected nodes with the above characteristics are defined as subaggressiveness nodes. However, this method does not mention which specific reputation model to select nor does it discuss how to combine with the specific reputation model and gives the corresponding test results. It also does not present the specific method of selecting standard time series parameters.

Reference [46] proposes a malicious node detection method based on online learning algorithm. This method first calculates the credibility of each path in the network according to the collected data packets, then models the path reputation obtained through online learning algorithm, and calculates the trust of each node, and detects malicious nodes through the clustering algorithm. The collaboration-based malicious detection mechanism proposed by Ref. [47] includes a data trust module and a reputation calculation module, which ensures honest data communication and reduces the false positive rate of malicious nodes. Reference [48] proposes an effective malicious node detection scheme based on weighted trust, which can detect malicious nodes in clustered wireless sensor networks. By considering the false positive and false negative examples, the node behavior can be truly handled. Reference [49] proposes a method called perceptron based detection, which uses perceptron and K-means method to calculate the trust value of nodes and detect malicious nodes accordingly, and by optimizing the network routing, the detection accuracy is further improved. Reference [50] proposes a blockchain trust model for malicious node detection in wireless sensor networks. It uses the blockchain smart contract, the quadrilateral measurement and the positioning method of wireless sensor network to realize the detection of malicious nodes in the three-dimensional space.

Some common applications of trust are shown in Table 1.

As the sociologist Niklas Luhmann said, “Trust and integrity are necessary in our life, it makes the various components of society integrate into one.” Reputation and trust are playing an increasingly important role in human society. In addition, in multiagent systems, due to the uncertainty of agent behavior and in order to protect well-behaved entities from malicious entities, reputation and
trust mechanism have been widely adopted and used as a social method [51]. However, the reputation and trust mechanism cannot be simply attributed to security issues. Security is used to prevent an entity from foreign invasion, ensure that another entity is designated with the entity, ensure that the sender and receiver of the message are designated entities, and prevent information from being illegally obtained by other entities. In contrast, reputation and trust are complex and diversified issues. Reputation and trust not only play a role in decision-making but also provide powerful tools for the establishment of relationships among entities in the insecure real world [43]. The reputation and trust mechanism has become an important supplementary tool for many types of network security solutions.

6. Conclusions

Due to the lack of infrastructure, wireless sensor networks are vulnerable to a variety of attacks. Without adequate security and physical protection, the number and types of applications of wireless sensor networks will be greatly reduced. Therefore, the security problems of wireless sensor networks need to be solved. As an effective supplement to the traditional security mechanism, the reputation and trust mechanism has attracted the attention of scholars and gradually introduced into ad hoc wireless sensor networks. Nowadays, it has obtained extensive theoretical research and application research, such as the selection of trusted routing path, malicious node identification, and so on. The reputation and trust mechanism can effectively encourage nodes to cooperate and take certain measures to punish malicious behavior of nodes, which not only improves the performance of the network but also enhances the security of the network. In this paper, the security standards and security challenges in wireless sensor networks are discussed in detail. In addition, this paper also discusses the background, significance, concept, and characteristics of reputation and trust, the division and composition of reputation system, and the common applications of reputation and trust mechanism in wireless sensor networks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors would like to express their gratitude to the support and help from the Civil Aviation Information Technology Research Center of CAFUC. This work was partially supported by the Scientific Project of CAFUC.
under grant nos. JG2022-06 and J2022-042, Civil Aviation Professional Project under grant nos. 0252109 and MHJY2022038, Sichuan Education Reform Project under grant no. JG2021-521, Central University Education Reform Project under grant no. E2022078, and Sichuan Science and Technology Program under grant nos. 2022YPG0190 and 2022JDR0116.

References

[1] J. Lopez, R. Roman, and C. Alcaraz, “Analysis of security threats, requirement, technologies and standards in wireless sensor networks,” in Foundation of Security Analysis and Design V, pp. 289–228, Springer, Berlin, Germany, 2009.

[2] J. Li, L. Yu, J. Zhao, C. Luo, and J. Zheng, “TSTE: a time-variant stochastic trust evaluation model in social networks,” KSII Transactions on Internet and Information Systems, vol. 11, no. 6, pp. 3273–3308, 2017.

[3] N. Battat, A. Makhoul, H. Kheddouci, S. Medjahed, and N. Atouaouzoug, “Trust based monitoring approach for mobile ad hoc networks,” in Ad-Hoc, Mobile, and Wireless Networks, pp. 55–62, Springer, Cham, Switzerland, 2017.

[4] X. Wu, “A robust and adaptive trust management system for guaranteeing the availability in the internet of things environments,” KSII Transactions on Internet and Information Systems, vol. 12, no. 5, pp. 2396–2413, 2018.

[5] J. Peng, H. Zhou, Q. Meng, and J. Yang, “Big data security access control algorithm based on memory index acceleration in WSNs,” Journal on Wireless Communications and Networking, vol. 2020, no. 1, 2020.

[6] J. Y. Yu, E. Lee, S. R. Oh, Y. D. Seo, and Y. G. Kim, “A survey on security requirements for WSNs: focusing on the characteristics related to security,” IEEE Access, vol. 8, pp. 45304–45324, 2020.

[7] C. Huang, M. Ma, X. Liu, A. Liu, and Z. Zuo, “Unequal probability marking approach to enhance security of traceback scheme in tree-based WSNs,” Sensors, vol. 17, no. 6, p. 1418, 2017.

[8] M. S. Abdalzaher and O. Mutla, “Employing game theory and TDMA protocol to enhance security and manage power consumption in WSNs-based cognitive radio,” IEEE Access, vol. 7, pp. 132923–132936, 2019.

[9] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” Computer, vol. 35, no. 10, pp. 54–62, 2002.

[10] A. A. Pirzada and C. McDonald, “Establishing trust in pure ad-hoc networks,” in Proceedings of the 27th Australasian Conference on Computer Science, vol. 26, pp. 47–54, Dunedin, New Zealand, January, 2004.

[11] E. C. H. Ngai and M. R. Lyu, “Trust and clustering based authentication services in mobile ad hoc networks,” in Proceedings of the 24th International Conference on Distributed Computing Systems Workshops, pp. 582–587, Tokyo, Japan, March, 2004.

[12] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[13] Z. Wei, S. Yu, and W. Ma, “Defending against internal attacks in healthcare-based WSNs,” Journal of Healthcare Engineering, vol. 202110 pages, Article ID 2081246, 2021.

[14] Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: a secure hop-by-hop data aggregation protocol for sensor networks,” ACM Transactions on Information and System Security, vol. 11, no. 4, pp. 1–43, 2008.

[15] H. Chan, A. Perrig, B. Przydatek, and D. Song, “SIA: secure information aggregation in sensor networks,” Journal of Computer Security, vol. 15, no. 1, pp. 69–102, 2007.

[16] J. Cheng, J. Li, N. Xiong, M. Chen, H. Guo, and X. Yao, “Lightweight mobile clients privacy protection using trusted execution environments for blockchain,” Computers, Materials & Continua, vol. 65, no. 3, pp. 2247–2262, 2020.

[17] S. Kaur and V. K. Joshi, “Hybrid soft computing technique based trust evaluation protocol for wireless sensor networks,” Intelligent Automation & Soft Computing, vol. 26, no. 2, pp. 217–226, 2020.

[18] L. Sun, C. Yu, D. Peng, S. Subramani, and X. Wang, “Fogmed: a fog-based framework for disease prognosis based medical sensor data streams,” Computers, Materials & Continua, vol. 66, no. 1, pp. 603–619, 2020.

[19] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, “A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks,” in Proceedings of the 25TH IEEE International Conference on Computer Communications, pp. 1–13, Rennes, France, April, 2006.

[20] C. Jia, L. Xie, X. Gan, W. Liu, and Z. Han, “A trust and reputation model considering overall peer consulting distribution,” IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 42, no. 1, pp. 164–177, 2012.

[21] N. Poolsappasit, M. Busby, and S. K. Madria, “Trust management of encrypted data aggregation in a sensor network environment,” in Proceedings of the IEEE 13th International Conference on Mobile Data Management, pp. 157–166, Bengaluru, India, November, 2012.

[22] C. R. Perez-Toro, R. K. Panta, and S. Bagchi, “RDAS: reputation-based resilient data aggregation in sensor network,” in Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1–9, Boston, MA, USA, July, 2010.

[23] H. Feng, G. Li, W. Lu, and L. Huang, “Trust based secure in-network data processing schema in wireless sensor networks,” Journal of Networks, vol. 6, no. 2, pp. 295–302, 2011.

[24] Y. Ni, L. Tian, and X. Shen, “The research of dynamic data fusion based-on node behavior trust for WSNs,” in Proceedings of the International Conference on Computer Design and Applications, pp. 534–538, Qinhuangdao, China, June, 2010.

[25] G. P. Gupta, M. Misra, and K. Garg, “Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks,” Journal of Network and Computer Applications, vol. 41, pp. 300–311, 2014.

[26] H. Alzaid, E. Foo, and J. G. Nieto, “RSDA: reputation-based secure data aggregation in wireless sensor networks,” in Proceedings of the 9th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 419–424, Dunedin, New Zealand, December 2008.

[27] C. Liu, Y. Liu, and Z. Zhang, “Improved reliable trust-based and energy-efficient data fusion for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 9, no. 5, pp. 1–11, 2013.

[28] Z. Taghiikhaki, N. Meratnia, and P. J. M. Hovinga, “Energy-efficient Trust-based aggregation in wireless sensor networks,” in Proceedings of the IEEE Conference on Computer Communications Workshops, pp. 584–589, Shanghai, China, April 2011.

[29] Z. Chen, L. Tian, and C. Lin, “Trust model of wireless sensor networks and its application in data fusion,” Sensors, vol. 17, no. 4, p. 703, 2017.
[30] H. Lin, S. Garg, J. Hu, X. Wang, M. J. Piran, and M. S. Hossain, “Data fusion and transfer learning empowered granular trust evaluation for Internet of Things,” *Information Fusion*, vol. 78, pp. 149–157, 2022.

[31] S. Baskar, R. Selvaraj, V. M. Kuthadi, and P. M. Shakeel, “Attribute-based data fusion for designing a rational trust model for improving the service reliability of internet of things assisted applications in smart cities,” *Soft Computing*, vol. 25, no. 18, pp. 12275–12289, 2021.

[32] K. Wang, C. M. Chen, Z. Liang et al., “A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain,” *Information Fusion*, vol. 72, pp. 100–109, 2021.

[33] Z. Liu, J. Ma, J. Weng et al., “LPPTE: a lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications,” *Information Fusion*, vol. 73, pp. 144–156, 2021.

[34] L. Yang, J. M. Kizza, A. Cemerlic, and F. Liu, “Fine-grained reputation-based routing in wireless ad hoc networks,” in *Proceedings of the IEEE Intelligence and Security Informatics*, pp. 75–78, New Brunswick, NJ, USA, May, 2007.

[35] B. Su, C. Du, and J. Huan, “Trusted opportunistic routing based on node trust model,” *IEEE Access*, vol. 8, pp. 163077–163090, 2020.

[36] H. Hu, Y. Han, H. Wang, M. Yao, and C. Wang, “Trust-aware secure routing protocol for wireless sensor networks,” *ETRI Journal*, vol. 43, no. 4, pp. 674–683, 2021.

[37] P. P. Jadhav and S. D. Joshi, “Atom search sunflower optimization for trust-based routing in internet of things,” *Int J Numer Model*, vol. 34, no. 3, Article ID e2845, 2021.

[38] G. Yin, G. Yang, Y. Wu, X. Yu, and D. Zuo, “A novel reputation model for malicious node detection in wireless sensor network,” in *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, Dalian, China, October 2008.

[39] K. F. Ssu, C. H. Chou, and L. W. Cheng, “Using overhearing technique to detect malicious packet modifying attacks in wireless sensor networks,” *Computer Communications*, vol. 30, no. 11-12, pp. 2342–2352, 2007.

[40] P. Reindl, K. Nygard, and X. Du, “Defending malicious collision attacks in wireless sensor networks,” in *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 771–776, Washington, DC, December, 2010.

[41] K. Hajiee, M. Fartash, and N. Osati Eraghi, “An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique,” *Neural Processing Letters*, vol. 53, no. 4, pp. 2829–2852, 2021.

[42] G. V. Crosby, L. Hester, and N. Pissinou, “Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks,” *International Journal on Network Security*, vol. 12, no. 2, pp. 107–117, 2009.

[43] S. Buchegger and J. Boudec, “Performance analysis of the CONFIDANT protocol,” in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, pp. 226–236, Lausanne, Switzerland, June, 2002.

[44] I. Pinyol and J. Sabater-Mir, “Computational trust and reputation models for open multi-agent systems: a review,” *Artificial Intelligence Review*, vol. 40, pp. 1–25, 2013.