Research on Trust-Based Secure Routing in Wireless Sensor Networks
Jing Liu¹*, Feng Xub
¹abCollege of Computer Science And Technology, Nanjing University of Aeronautics and Astronautics, NanJing, China;
* Corresponding author: 18751953271@163.com

ABSTRACT
In the wake of developments in science and technology, wireless sensor networks have attracted more and more researchers. Compared with traditional networks, wireless sensor networks are very different in many respects. Energy saving, security and reliability are the most concerned topics of wireless sensor networks. As the network expanded scale and complexity are increasing, the limited sensor node resources and the uncertainty of the environment layout, the traditional security mechanism is no longer applicable to wireless sensor networks. This article reviews the common assault forms, security technologies and security mechanisms of trust based routing protocols proposed in wireless sensor networks in recent years. Based on the analysis of various types of attacks, the development direction of the trust mechanisms in wireless sensor networks is provided.

Keywords: Wireless sensor network, routing protocol, trust mechanism

1. INTRODUCTION
Wireless sensor network (WSN) is a distributed sensor network in which sensor nodes communicate wirelessly [1]. In recent years, wireless sensor networks (WSNS) have attracted more and more attention due to their versatility. Sensor nodes can monitor or sense physical attributes such as weather, pressure, humidity and other environmental data, process the data, and transmit the data to a base station or receiver. These characteristics of nodes and wireless connection mode broaden the application prospect of wireless sensor networks, including military, ecological environment monitoring, intelligent transportation and other fields. Generally, the network is static and battery-powered, and these nodes are arranged in large numbers in areas lacking connectivity and wired Internet infrastructure to monitor or track events [2]. Once deployed, it can work without human interference.

The wireless sensor network has several characteristics different from the traditional network[3]: (1) the sensor node is powered by the battery, the energy is low, and should not be replaced; (2) The computing capacity of the processor of the node is low, so it cannot support algorithms with a large amount of computation; (3) The storage capacity of the node is limited and does not support the storage of large amounts of data; (4) Sensor networks tend to deploy a large number of sensor nodes, which are easily affected by environmental factors, resulting in changes in network topology.

Security is one of the most concerned performance indicators in the design of wireless sensor networks. Therefore, this paper summarizes the common types of attacks in wireless sensor networks and the preventive measures used to resist these attacks by studying various types of trust-based security mechanism routing protocols.

2. OVERVIEW OF ATTACK TYPES
Most of the attacks targeted wireless sensor networks are based on the energy constrained nature of sensor nodes[4]. Sensor energy is exhausted by various attack means, which makes the energy of network nodes fail prematurely, thus destroying the whole network structure and paralyzing the wireless sensor network. Due to its own characteristics, wireless sensor networks are vulnerable to various types of attacks, as shown in Figure 1:
Figure 1. Common attack.

2.1 Obtain Network Data

The intrusion node usually has legitimate identity information and is a trusted common node for its neighbor nodes. When the neighbor nodes near the intrusion node communicate wirelessly, it can obtain the communication data of the neighbor nodes by means of signal monitoring.

Monitoring [5]: it focuses on stealing information. Since the radio frequency communication is the way of data transmission in most wireless sensor networks, attackers can steal information in the network through monitoring channels, so as to achieve the purpose of attack.

2.2 Tamper Network Data

Replication Attack [6]: After capturing some sensor nodes, the attacker can obtain the information stored in the nodes through reverse operation, and even make a lot of replication nodes to be arranged in the field of the captured nodes. The replication node deployed in the network can inject wrong data into the network and also obtain the sensing data in the network.

Sinkhole Attack [7]: By spreading forged routing information in the network, the attacking node pretends to be the node responsible for data forwarding in the network.

2.3 Jamming Communication

The attacker is not satisfied with external wireless interference, but wants to interfere and block some nodes and data in the network. For example, by sending a large amount of communication data to occupy the channel or the communication window of the node.

Flooding Attack [8]: The principle of flooding attack is that the attacker sends a large number of communication requests or data to a node or several nodes in the network. As a result, the attacked node cannot process normal data sending and receiving in the network due to resource exhaustion.

Sybil Attack [9]: Sybil attack are well known in peer-to-peer, wired, and wireless network environments. The malicious nodes disguise themselves to gain the favor of neighboring nodes, and declare to other members that they have multiple identities.

Selective Forwarding [10]: Under this type of attack, the attacker captures the sensor node through decryption and other means, which is different from the normal node in completely forwarding data packets. On the contrary, it forwards some unimportant data selectively or discards data packets directly to destroy the network.

2.4 Attack And Control Network

When an invading node completes a wormhole attack or a black hole attack, it becomes a node with certain privileges. It can make use of these advantages to carry out more in-depth attacks, such as controlling some nodes to complete attacks and hide themselves as hosts.
Wormhole Attack [11]: Wormhole attack is usually launched by two or more malicious nodes working together. By publishing forged routing information, the path between malicious nodes is far less than its true path distance.

3. SECURITY MECHANISMS

3.1 Key Management

The encryption technology is considered from the aspect of data security, and it also plays a fundamental role in the application of wireless sensor networks.

Centralized Key Management [12]: The key is generated, stored, archived, backed up and recovered in a centralized manner. This method mainly refers to work based on the Key Distribution Center (KDC, such as SPINS.

Distributed Key Management [13]: Decentralized key management is the key to solve blockchain private key management. The private key is hosted to a decentralized network protocol and shared securely among specified users. This method mainly uses the key pre distribution scheme. The most typical representative of this management mode is E-G.

3.2 Secure Routing Protocol Design

Security and energy consumption are two topics of concern in wireless sensor networks. In recent years, most researches are about the improvement of energy consumption. The improvement of security will increase the complexity of routing protocol design, so it is difficult. However, given the security mechanisms, energy balance issues can be better assessed.

Combined with several security mechanisms: At present, the relatively complete security mechanisms include: key management, authentication technology, timestamp mechanism and reputation mechanism. For example, use reputation evaluation in WSN. This node is used to evaluate the behavior of adjacent nodes or use the base station for monitoring and detection. The improved routing protocol can effectively resist sybil attack, worm attack and selective attack.

3.3 Intrusion Detection System

In the analysis of intrusion detection in wireless sensor networks, the research of intrusion detection architecture is the foundation. Its design process and functions must be specific to specific scenarios.

Distributed detection system [14]: Distributed detection system is a model proposed earlier, which is mostly applied in the planar network. By adding detection algorithm to independent nodes, it determines whether there is intrusion behavior according to the data it monitors, and reports the intrusion behavior to the Sink node after discovering it.

The advantages of this detection system are simple, convenient, easy to deploy, adaptive ability and fault tolerance. The disadvantages are also obvious. Single node detection consumes a lot of communication resources, storage resources and energy, and a single node needs to have strong processing power to run a complete detection algorithm.

4. TRUST-BASED ROUTING PROTOCOL

Trust is a subjective view of the reliability of other entities or functions, including connectivity of path, veracity of data, processing capability of node and availability of service etc.

4.1 Early Research

In the early literature, trust based routing protocols were improved on the basis of current protocols and used some special methods to deal with trust factors, including EETA [15], ATRM [16], etc. With more and more research on trust, more improved models of trust based routing have emerged. Security issues are considered more comprehensively by combining different attributes, including LEACH-TM [17], etc.

In [18], This literature is a classic distributed trust model, which specifies that each node in the network observes the historical interaction behavior of neighboring nodes during network operation, and evaluates the trust value of neighboring nodes according to their historical non cooperative behavior.

In [19], A secure routing mechanism based on trust awareness is proposed. Its trust calculation consists of direct trust value, indirect trust value and incentive factor. The node takes the direct trust of the neighbor node as the recommended trust value, and the average recommended trust value of the neighbor node as the indirect trust value of the node.
In [20], a hierarchical routing algorithm based on node trust value is proposed. The member node with the largest trust value is selected as the shadow cluster head, and the subsequent trust evaluation is required to be completed by the shadow cluster head. Only the node inspected by the shadow cluster head can communicate with the cluster head. However, improvements are still needed in terms of energy consumption.

In [21], a routing protocol based on cooperative awareness for low energy consumption wireless sensor networks is proposed. This protocol evenly deploys trust evaluation nodes in the network, so that the energy consumption of trust evaluation nodes in the network is relatively consistent. At the same time, the trust evaluation nodes evaluate each other, send the evaluation results to their corresponding cluster heads, and route to the sink node through the cluster heads. The sink node calculates the trust value of the evaluation node and decides whether to update the evaluation node.

In [22], this paper proposes a mechanism for adjacent nodes to exchange trust information, which can maintain the trust information between adjacent sensor nodes. Its purpose is to prevent attack nodes from being selected as cluster heads. Although the algorithm is robust to malicious node attacks, it is vulnerable to selective forwarding attacks.

The comparison experiment uses the same energy consumption model as LEACH. This model only calculates the energy consumed by the communication between nodes, not the energy consumed in the data processing of each node. The calculation formula of one-to-one trust value is as follows:

\[ E_{\text{elec}} = 50nJ / \text{bit} \]  
\[ E_{\text{amp}} = 100pJ / \text{bit} / m^2 \]  

The energy consumption of data transmission between nodes is positively correlated with the distance \( d \). When \( d \) reaches a threshold \( d_0 \), the energy consumption increases exponentially.

When \( d < d_0 \): The energy consumption calculation adopts the free space channel model [25], that is, the communication energy consumption between nodes has a linear relationship with \( d^2 \), and the power amplification factor is:

\[ E_{\text{fs}} = 10pJ / \text{bit} / m^2 \]  

When \( d > d_0 \): The energy consumption calculation adopts the multi-path attenuation model, that is, the communication energy consumption between nodes has a linear relationship with \( d^4 \), and the power amplification factor is:

\[ E_{\text{mp}} = 0.0013pJ / \text{bit} / m^2 \]  

According to the above parameter settings, when a data packet of size \( k \) is sent to the node, the energy consumption \( E_{\text{TX}} \) is:

\[ E_{\text{TX}}(k,d) = \begin{cases} E_{\text{elec}} \cdot k + E_{\text{fs}} \cdot k \cdot d^2, & d < d_0 \\ E_{\text{elec}} \cdot k + E_{\text{mp}} \cdot k \cdot d^4, & d \geq d_0 \end{cases} \]  

When a node receives a data packet of size \( k \), the energy consumption \( E_{\text{RX}} \) is:

\[ E_{\text{RX}}(k,d) = E_{\text{elec}} \cdot k \]
Figure 2 is a comparative experimental diagram of the energy consumption of five protocols in the literature 23-27 under the same attack environment. Since Literature 23 is a combination of trust based routing module and trust management module, it is not ideal in terms of energy consumption. Literature 26 is a framework based on distributed trust, so its energy consumption is relatively low.

4.2 Recent Research

In recent years, wireless sensor networks have gradually become a research hotspot, and more and more research has been done on secure routing in wireless sensor networks. This section summarizes some work in this field in recent years, and analyzes methods, trust measurement, innovation, complexity, advantages and disadvantages. Table 1 analyzes the protocols proposed in recent years.

In [23], the cluster head node selects some surveillance nodes to calculate reputation and trust routes. Monitoring mechanism and anomaly detection mechanism based on energy threshold are used to detect errors generated by the attacked node or invalid data. This study ignored the trust rating of CH, which is an obvious disadvantage of this plan.

In [24], a reputation based low-power routing mechanism (ERRM) is proposed, which calculates the reputation of adjacent nodes. Data aggregation is performed through the median reputation collected by node lookup. Judge whether the aggregation result exceeds the threshold value. If it exceeds the threshold value, the reputation value will be discarded, and then the rest of the reputation value will be weighted to average. Finally, the weighted reputation will be obtained. The main advantage of this mechanism is that data and data sequences are not easy to be damaged by malicious nodes when they arrive at the base station.

In [25], this paper proposes a new security aware routing protocol for wireless sensor networks, which combines multiple attributes of sensor nodes in data communication, residual energy and trust recommendation. The proposed trust model considers the impact of attack frequency and improved sliding time window. The protocol can deal with attacks from trusted nodes well. However, the disadvantage is that the cluster head selection of trust awareness is ignored.

In [26], a trust based low-power routing protocol (TEESR) is proposed, which uses an authorization mechanism to reduce the probability of multiple malicious nodes in adjacent areas. The node trust value determines the coverage radius and multi-path security route, and then the cluster head and the base station node make a comprehensive judgment to select the route with higher security value. Although the proposed protocol performs well in dealing with external attacks, such as convergence holes and wormholes, it is powerless to deal with internal attacks.

In [27], a new trust aware secure routing protocol (TSRP) is proposed to prevent wormhole, selective forwarding and black hole attacks. The protocol has good performance in average packet loss rate and throughput, but high energy consumption is a disadvantage.

In [28], aiming at the uncertain factors in trust management, a fuzzy trust model is proposed to deal with such problems, which is commonly used in decision control systems. The most basic feature of trust based sensor networks is uncertainty, because the evidence to be supported may be fuzzy, or the strategy to be implemented may be fuzzy.
### Table 1. Trust-based Routing Protocol.

| Protocol | Method | Advantage and Limitation |
|----------|--------|--------------------------|
| [18]     | Combination of trust-based routing module and trust management module. | Prolong network life. High energy consumption. |
| [19]     | Route is determined by location, trust value and energy. | Easy to deploy. The types of attacks that can be solved are limited. |
| [20]     | Each node generates a reputation value based on its parent node and child node. | Robust and efficient in detecting Flooding Attack. High energy consumption. |
| [21]     | A framework based on distributed trust and used to select cluster heads with high trust values. | Reduce the probability of malicious nodes being selected as cluster heads. Less emphasis on trust assessment. |
| [22]     | Trust management module maintains trust information between all nodes. | Robust performance against malicious nodes. Vulnerable to collusion attacks. |
| [23]     | Reputation and trust are computed by the surveillance node. | Less energy consumption. The trust rating of cluster heads is ignored. |
| [24]     | The aggregation is done by finding the median of the collected reputation. | High success rate. High cost computation. |
| [25]     | Establish reliable routing based on data communication, data, residual energy and recommended trust evaluation. | Works well when dealing with various routing and trusted node attacks. Does not include the trust-aware cluster head selection mode. |
| [26]     | Multipath secure routing based on node trust values. | Resist sinkhole attack and wormhole attack. Unable to defend against internal attacks. |
| [27]     | The base station calculates the trust values of all nodes and establishes multiple paths with different security degrees. | Performance well in average packet loss ratio and throughput. High energy consumption. |
| [28]     | Fuzzy trust model to handle the uncertainty. | Less energy consumption. Choosing the appropriate time interval is difficult. |

### 5. CONCLUSION

This paper reviews the trust mechanisms in wireless sensor networks and the corresponding attacks and countermeasures. For different application scenarios of wireless sensors, we give the motivation behind the application of trust schemes. First, we classify all attacks related to trust mechanism in wireless sensor networks. Secondly, we analyze the design ideas of various trust schemes, and emphasize the opportunities and challenges of trust schemes in wireless sensor networks. Finally, by summarizing the optimized trust mechanisms in wireless sensor networks, we conducted an extensive literature survey. Our research result is that the trust evaluation mechanism algorithm combined with data information encryption, fuzzy set theory and other security plans to guarantee that the security measures of wireless sensor networks are trustworthy. At the same time, it is clear from these papers that reducing energy consumption while ensuring safety is a research hotspot in the future.
REFERENCES

[1] Yu Y, Li K, Zhou W, et al. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures[J]. Journal of Network and computer Applications, 2012, 35(3): 867-880.

[2] Ishmanov F, Bin Zikria Y. Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues[J]. Journal of Sensors, 2017, 2017.

[3] Bhola J, Soni S, Cheema G K. Recent trends for security applications in wireless sensor networks—a technical review[C]/2019 6th international conference on computing for sustainable global development (INDIACom). IEEE, 2019: 707-712.

[4] Khare A, Gupta R, Shukla P K. Improving the protection of wireless sensor network using a black hole optimization algorithm (BHOA) on best feasible node capture attack[M]/IoT and Analytics for Sensor Networks. Springer, Singapore, 2022: 333-343.

[5] Prasanna S, Rao S. An overview of wireless sensor networks applications and security[J]. International Journal of Soft Computing and Engineering, 2012, 2(2): 2231-2307.

[6] Manjula V, Chellappan C. The replication attack in wireless sensor networks: Analysis and defenses[C]/International Conference on Computer Science and Information Technology. Springer, Berlin, Heidelberg, 2011: 169-178.

[7] Kibirige G W, Sanga C. A survey on detection of sinkhole attack in wireless sensor network[J]. arXiv preprint arXiv:1505.01941, 2015.

[8] Singh V P, Jain S, Singhai J. Hello flood attack and its countermeasures in wireless sensor networks[J]. International Journal of Computer Science Issues (IJCSI), 2010, 7(3): 23.

[9] Dhamodharan U S R K, Vayanaperumal R. Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method[J]. The Scientific World Journal, 2015, 2015.

[10] Bysani L K, Turuk A K. A survey on selective forwarding attack in wireless sensor networks[C]/2011 International Conference on Devices and Communications (ICDeCom). IEEE, 2011: 1-5.

[11] Govindasamy J, Punniakody S. A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack[J]. Journal of Electrical Systems and Information Technology, 2018, 5(3): 735-744.

[12] Liu J, Tong X, Wang Z, et al. A centralized key management scheme based on McEliece PKC for space network[J]. IEEE Access, 2020, 8: 42708-42719.

[13] Hao Y, Cheng Y, Zhou C, et al. A distributed key management framework with cooperative message authentication in VANEts[J]. IEEE Journal on selected areas in communications, 2011, 29(3): 616-629.

[14] Guo X, He Y, Atapattu S, et al. Power allocation for distributed detection systems in wireless sensor networks with limited fusion center feedback[J]. IEEE Transactions on Communications, 2018, 66(10): 4753-4766.

[15] Alrajeh N A, Khan S, Shams B. Intrusion detection systems in wireless sensor networks: a review[J]. International Journal of Distributed Sensor Networks, 2013, 9(5): 167575.

[16] Liu K, Abu-Ghazaleh N, Kang K D. Location verification and trust management for resilient geographic routing[J]. Journal of parallel and distributed computing, 2007, 67(2): 215-228.

[17] Lewis N, Foukia N. An efficient reputation-based routing mechanism for wireless sensor networks: Testing the impact of mobility and hostile nodes[C]/2008 Sixth Annual Conference on Privacy, Security and Trust. IEEE, 2008: 151-155.

[18] Li Y Z, Zhang A L, Liang Y Z. Improvement of leach protocol for wireless sensor networks[C]/2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control. IEEE, 2013: 322-326.

[19] Ganeriwal S, Kansal A, Srivastava M B. Self aware actuation for fault repair in sensor networks[C]/IEEE International Conference on Robotics and Automation, 2004. Proceedings. ICRA'04. 2004. IEEE, 2004, 5: 5244-5249.

[20] Zahariadis T, Trakadas P, Leligou H C, et al. A novel trust-aware geographical routing scheme for wireless sensor networks[J]. Wireless personal communications, 2013, 69(2): 805-826.

[21] Srinivasan A, Wu J. Secure and reliable broadcasting in wireless sensor networks using multi-parent trees[J]. Security and Communication Networks, 2009, 2(3): 239-253.

[22] Song F, Zhao B. Trust-based LEACH protocol for wireless sensor networks[C]/2008 Second International Conference on Future Generation Communication and Networking. IEEE, 2008, 1: 202-207.

[23] Ahmad F, Kurugollu F, Kerrache C A, et al. NOTRINO: a NOvel hybrid TRust management scheme for INternet-Of-vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 70(9): 9244-9257.

[24] Lewis N, Foukia N. An efficient reputation-based routing mechanism for wireless sensor networks: Testing the impact of mobility and hostile nodes[C]/2008 Sixth Annual Conference on Privacy, Security and Trust. IEEE, 2018: 151-155.

[25] Sun B, Li D. A comprehensive trust-aware routing protocol with multi-attributes for WSNs[J]. IEEE Access, 2017, 6: 4725-4741.

[26] Ilyas M, Ullah Z, Khan F A, et al. Trust-based energy-efficient routing protocol for Internet of things–based sensor networks[J]. International Journal of Distributed Sensor Networks, 2020, 16(10): 1550147720964358.

[27] Hu H, Han Y, Wang H, et al. Trust-aware secure routing protocol for wireless sensor networks[J]. ETRI Journal, 2021, 43(4): 674-683.

[28] Boukerche A, Ren Y. A trust-based security system for ubiquitous and pervasive computing environments[J]. Computer communications, 2008, 31(18): 4343-4351.