JST: Smart Systems and Devices
Volume 33, Issue 1, January 2023, 017-024

Classification of Secure Routing Protocols in Wireless Sensor Networks

Long Tran Huy[1*], Chinh Tran Thien[1], Hoai Trung Tran[2]
[1]*Research Institute of Posts and Telecommunications, Ha Noi, Vietnam*
[2]*University of Transport and Communications, Ha Noi, Vietnam*
[*]*Corresponding author email: huylong.ript@gmail.com*

Abstract

A wireless sensor network (WSN) is a collection of wirelessly connected multifunction sensor devices (referred to as wireless sensor nodes) in an area that requires sensing. In WSNs, wireless sensor nodes have a short transmission range, and processing capacity, storage, and power supply to the node are also limited. In addition, WSNs often include a significant number of sensor nodes, deployed in a large area to meet the requirements set forth, and communication in WSNs must be through multi-hop communication connections. Therefore, the secure routing protocols (SRPs) in WSNs are responsible for finding and maintaining secure and reliable connection routes and are especially energy-efficient (because the wireless sensor node is limited in terms of the power supply). Therefore, energy-efficient routing, as well as secure communication and data transmission between wireless sensor nodes are fundamental challenges for providing security services in WSNs. Currently, many energy-efficient and SRPs in WSNs have been proposed. In this paper, we synthesize the classification and arrangement of energy-efficient and SRPs, as well as provide a method to calculate attack probability (AP) for secure routing in WSN.

Keywords: WSNs, secure, routing, protocols, energy-efficient, classification, SRPs.

1. Introduction

In recent years, with the strong development of wireless communication, WSNs have made great leaps forward, due to being applied in many different fields such as civil, military, medical, environmental and traffic monitoring, science, etc. WSNs have an architecture of many wireless sensor nodes that communicate with each other using radio frequencies as shown in Fig. 1, [1].

In WSNs, these wireless sensor nodes are resource-constrained devices characterized by low processing power, narrow bandwidth, limited battery capacity, and memory. The main task of the wireless sensor node is to sense and collect data from a certain area, process and transmit them to the sink node where the applications are located [2]. The basic architecture of a wireless sensor node as shown in Fig. 2, consists of the main components: a sensor, an analog-to-digital converter, a small microprocessor (including processor and memory), a locator, a radio transceiver (transmitter and receiver) and a small battery (power supply) to power for this wireless sensor node [3].

In WSNs, the communication between wireless sensor nodes and base stations (BS) is done through the so-called protocol stack consisting of five layers as shown in Fig. 3: the physical layer, data link layer, network layer, transport layer, and application layer. Specifically: 1) The physical layer performs the tasks of selecting communication frequencies, generating carrier frequencies, modulating signals, encrypting data security, ...; 2) The data link layer performs data frame detection, data stream multiplexing, medium access, and error control to achieve consistent point-to-point and point-to-multipoint connectivity; 3) The network layer performs the task of routing the data delivered by the transport layer; 4) The transport layer is responsible for holding the data stream; 5) The application layer performs the task of adapting its content to the characteristics of each specific application [1].

In addition, the protocol stack also includes 5 management planes to optimize the performance of WSNs in terms of respective performance metrics. Specifically: i) The Mobility Management Plane is responsible for maintaining the data routes even in the presence of mobility of the nodes; ii) The power management plane is responsible for reducing energy consumption; iii) The task management plane is responsible for assigning sensing, routing, and data aggregation tasks, to the sensor nodes; iv) The Quality of Service (QoS) management plane is responsible for managing fault tolerance, controlling errors, and optimizing performance against specific QoS metrics; v) The security management plane is responsible for recording and regulating network activity in terms of security [4].

ISSN: 2734-9373
https://doi.org/10.51316/jst.163.ssad.2023.33.1.3
Received: September 9, 2022; accepted: November 11, 2022

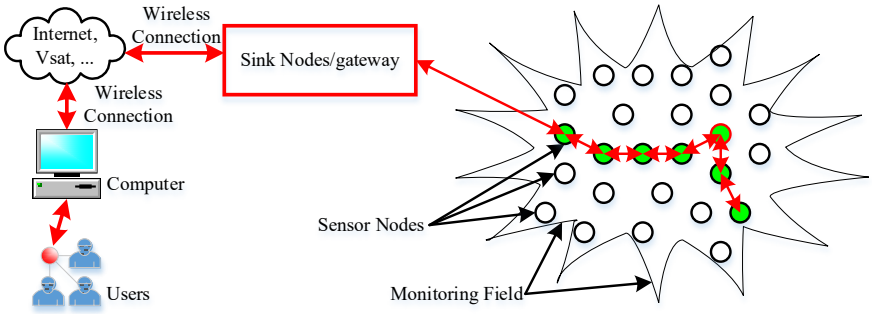

Fig. 1. The architecture of the components of the wireless sensor networks

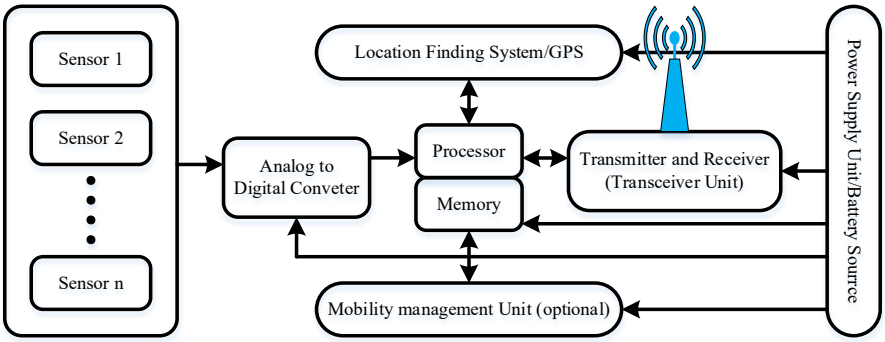

Fig. 2. Wireless sensor node architecture

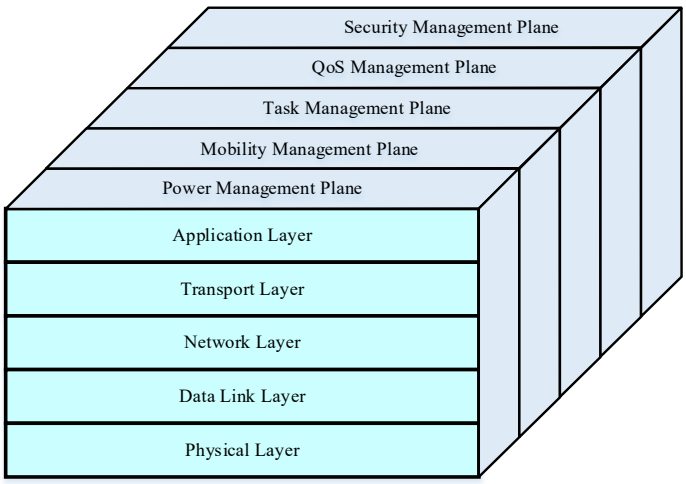

Fig. 3. Protocol stacks in WSNs

A WSN can have one or more BSs along with hundreds or even thousands of wireless sensor nodes. This makes that WSNs can be deployed for many beneficial applications such as environmental monitoring, traffic control, object tracking, inventory control, fire detection, diagnostics, and damage identification. surveillance and reconnaissance, and various military applications [1]. However, there are also serious problems such as congestion, connection loss, security, sensitivity to attacks, QoS degradation, and limited coverage, [5-10].

The purpose of the article is to present the classification of routing protocols in WSNs with both classical and new modern protocols. The content presented in the article provides an updated and more comprehensive survey of energy-saving and SRPs in WSNs. Accordingly, the remainder of this article is organized as follows. Part 2, summarizes and presents

the classification of SRPs in WSNs by Christos Nakas, [1]; by Vivek Sharma and Devershi Pallavi Bhatt [3]; by Shio Kumar Singh, [11]; by Vikas Bhandary, [12]; by Yasir Arfat and Riaz Ahmed Shaikh [13]; and by Bharat Bhushan and G. Sahoo [14]. In Sections 3, 4, and 5, we propose an analysis of the types of protocol routing in WSNs and possible applications of these routing routes, and finally, Section 6 is the conclusion.

2. Summary of Classification of SRPs in WSNS

2.1. Synthesize How to Classify SRPs according to Christos Nakas

The main SRPs in WSNs are classified under the survey in [1], including communication model-based SRPs, network structure-based SRPs, topology-based SRPs, and reliable-based SRPs. The communication model-based SRPs are further divided into query-based SRPs, coherent/non-coherent-based SRPs, and negotiation-based SRPs as follows:

- The network structure-based SRPs are further divided into flat energy-based SRPs, hierarchical-based SRPs, and topology-based SRPs;

+ Flat energy based SRPs are further subdivided into reactive flat SRPs, proactive flat SRPs, and hybrid flat SRPs;

+ Hierarchical-based SRPs are further subdivided into hierarchical-based SRPs, zone-based SRPs, and fuzzy logic-based SRPs;

- The topology-based SRPs are further divided into location-based SRPs, mobile agent-based SRPs, and mobile sink-based SRPs;

- The reliable-based SRPs are further divided into QoS-based SRPs and multipath-based SRPs.

2.2. Synthesize How to Classify SRPs according to Vivek Sharma and Devershi Pallavi Bhatt

Under the review in [3], the main SRPs in WSNs are classified, according to their application features including flood-based SRPs, hierarchical-based SRPs, data-centric-based SRPs, location-based SRPs, and QoS-based SRPs.

2.3. Synthesize How to Classify SRPs according to Shio Kumar Singh

The main SRPs in WSNs are classified according to routing protocols in [11], including location-based SRPs, data-centric-based SRPs, hierarchical-based SRPs, mobility-based SRPs, multipath-based SRPs, and heterogeneity-based SRPs, and QoS-based SRPs.

2.4. Synthesize How to Classify SRPs according to Vikas Bhandary

The main SRPs in WSNs are classified under the protocols in [12], including QoS-based SRPs, swarm intelligence-based SRPs, and network structure-based SRPs as follows:

- The QoS-based SRPs are further divided into latency constrained-based SRPs and multi-constrained-based SRPs. Specifically;

- The swarm intelligence-based SRPs;

- The network structure-based SRPs are further divided into flat network-based SRPs, hierarchical network-based SRPs, and location-based SRPs.

2.5. Synthesize How to Classify SRPs according to Yasir Arfat and Riaz Ahmed Shaikh

The main SRPs in WSNs are classified under the protocols survey in [13], including cluster-based SRPs and non-cluster-based SRPs as follows:

- The cluster-based SRPs are further divided into cluster-based SRPs that use symmetric key cryptography, asymmetric key cryptography, and hybrid key cryptography;

- Non-cluster-based SRPs are further divided into non-cluster-based SRPs that use symmetric key cryptography, asymmetric key cryptography, and hybrid key cryptography.

2.6. Synthesize how to Classify SRPs according to Bharat Bhushan and G. Sahoo

The main SRPs in WSNs are classified under the routing protocols in [14] including the flat network-based SRPs, the hierarchical network-based SRPs, and the QoS aware-based SRPs as follows:

- The flat network-based SRPs are further divided into reactive-based SRPs, proactive-based SRPs, and hybrid-based SRPs;

- The hierarchical-based network SRPs are further divided into chain-based hierarchical SRPs, grid-based hierarchical SRPs, tree-based hierarchical SRPs, area-based hierarchical SRPs, and other miscellaneous-based hierarchical SRPs;

- The QoS aware-based SRPs.

3. Method for Classification of SRPs in WSNs

WSNs based on sensor nodes (SNs) are applied to monitor, collect and report events depending on the application domain. However, SNs are often limited in terms of power supply, computational capacity and transmission bandwidth, and also require a more efficient method of forwarding and processing data. Therefore, in order to prolong the life of the SN or maintain the long-term survival of the WSNs, it is necessary to apply efficient routing protocols to detect and maintain the transport routes in the network. But the suitability of a particular routing protocol depends on the capabilities of the SNs and diverse application requirements. Therefore, in the following, we introduce a general method for classifying of SRPs in WSNs.

SRPs are classified as node-centric, data-centric, location-aware and QoS-based routing protocols. Most SRPs in ad-hoc networks are node-centric protocols, where destinations are assigned based on the numerical addresses (or identifiers) of SNs.

In WSNs, central communication is not the type of communication that is usually expected. Therefore, routing protocols for WSNs are often data-centric or location-aware. In data-centric routing, the sink node sends queries to certain regions and acquires data from SNs located in the selected regions. Since data is being requested through queries, attribute-based classification of SRPs is necessary to specify the attributes of the data.

At the same time, SRPs also need to be classified based on the sensor network architecture [15]. Some WSNs include homogeneous nodes, while others include heterogeneous nodes. Based on this concept, we can classify protocols whether they are operating on flat topology or hierarchical topology. In flat routing protocol all nodes in the network are treated equally. The Hierarchical Routing Protocol is a natural approach to apply to heterogeneous networks where some SNs are stronger than others.

4. Proposed Classifications of SRPs in WSNs

Based on synthesizing ways of classifying routing protocols in WSNs of authors [1, 3] and [11-14], we propose to classify SRPs in WSNs into nine categories as follows (see Fig. 4): 1) Network structure-based SRPs; 2) Data-centric-based SRPs; 3) Mobility-based SRPs; 4) Multipath-based SRPs; 5) Heterogeneity-based SRPs; 6) QoS-based SRPs; 7) Cluster-based SRPs; 8) Swarm intelligence-based SRPs; 9) Communication model-based SRPs. The topology-based SRPs are classified as flat network-based SRPs, hierarchical network-based SRPs, and location-based SRPs; QoS-based SRPs are classified as latency constrained-based SRPs, and latency multiconstrained-based SRPs; Cluster-based SRPs are classified as cluster-based SRPs and non-cluster-based SRPs.

Moving on, secure rerouting protocols can be classified as flat network-based SRPs and further classified into proactive-based SRPs, reactive-based SRPs, and hybrid-based SRPs; hierarchical-based SRPs are classified as chain-based hierarchical SRPs, grid-based hierarchical SRPs, tree-based hierarchical SRPs, area-based hierarchical SRPs, and another miscellaneous-based hierarchical SRPs; Cluster-based SRPs and non-cluster-based SRPs is classified as using symmetric key cryptography and use asymmetric key cryptography and use hybrid key cryptography SRPs. Communication model-based SRPs are classified into query-based and coherent/non-coherent-based and negotiation-based SRPs.

Next, we propose to use some typical security routing protocols and attack types, as well as security solutions corresponding to types of attacks on the layer in WSN [1, 3], [11-14].

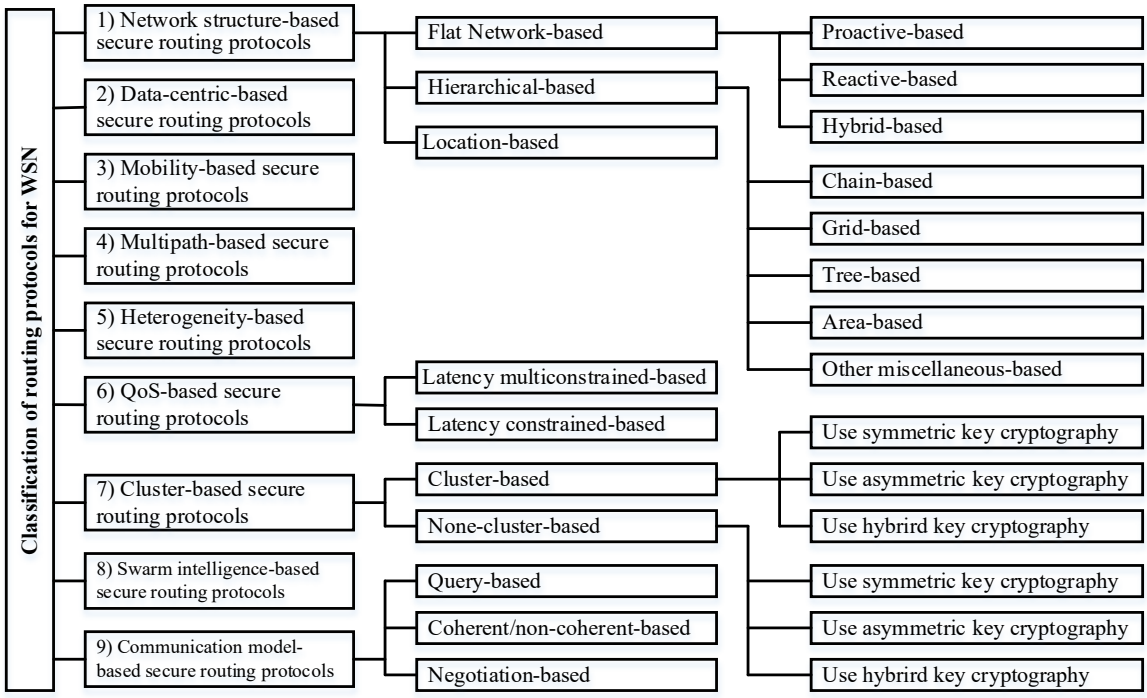

Fig. 4. Synthesize the proposed classification of secure routing protocols for WSNs

Table 1. Recommended to use some typical secure routing protocols

Attack on layers in WSN	Type of attacks	Recommended to use some typical secure routing protocols	Recommend using a security solutions
Attack on physical layer	Tampering, jamming, eavesdropping, routing traceback	TEESR, LEACH, CASER, SEAR, SCRA, GAF, GEAR, TBF, BVGF	Tamper-proofing, tampering monitoring software, spread spectrum, priority message, region mapping, mobile-agent based, defensive protocols, cryptographic techniques, detection strategies, symmetric key cryptography, lower duty cycle, region mapping, mode change
Attack on data link layer	Exhaustion, sinkhole, wormhole, black hole, unfairness, hello flooding, eavesdropping, sybil, collisions	TEESR, LEACH, CASER, SEAR, SCRA, SPIN, Directed Diffusion, Rumor, COUGAR, ACQUIRE, EAD, Information-Directed, Gradient- Based, Energy-aware, Information-Directed, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination, MECN, SPIN	Message authentication code (MAC), authentication, Protection from broadcast attacks, limitation of rate, nodes authentication, trust sensing protocols, packet authentication, monitor transmission, watchdog, symmetric key cryptography, error-correction code, rate limitation, small frames
Attack on network layer	Replay, sybil, sinkhole, blackhole, grayhole, wormhole, flooding, spoofed routing information, selective packet forwarding, hello flood, information disclosure, byzantine, resource depletion, DoS, altered, altering, acknowledgment spoofing	TEESR, LEACH, CASER, SEAR, SCRA, EEND, MRP, tSEL, SCMRP, Secure Directed Diffusion, HySEC, Nlog, TBRPF, TORA, Rumor, ZRP, H-LEACH, GAF, GEAR, TBF	Message authentication code (MAC), trust value management, intrusion detection mechanisms, malicious node detections and avoidance algorithms, lightweight encryption algorithms specially designed for WSN, Secure broadcasting and multicasting protocols, symmetric key cryptography, asymmetric key cryptography, hybrid, egress filtering, authentication, monitoring, redundancy checking, probing, using geographic and temporal information, bidirectional link authentication verification)
Attack on transport layer	Selective forwarding, Sybil attack, desynchronizatio, flooding, hello flood	Directed Diffusion, HySEC, Nlog, ZRP, H-LEACH, PEGASIS, GeRaF	Replication, probing, Identity tokens, authentication, multi-hoping, multipath routing, acknowledgments, pre-distribution validation of key, position verification, cryptography, hybrid, client puzzles
Attack on application layer	Repudiation and data corruption, overwhelming, malicious code	TEESR, LEACH, CASER, SEAR, SCRA, SEAD, TTDD, Joint Mobility, Data MULES, Dynamic Proxy Tree-Base Data Dissemination, Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery, APTEEN	Strong authentication schemes at application layer, secure firewall platforms, symmetric cryptography

5. Security Routing Attack Model in WSNs

According to Qiong Shi [15] (2020), secure routing is very important for WSNs because they are very vulnerable to attack. The authors proposed a new SRP for WSNs in the presence of malicious nodes, where the trust value and state of each relay node in the route are considered in the proposed SRP. The confidence value is defined as the node's Attack Probability *(AP)* according to previous packet forwarding behaviors, and state is a metric that combines residual energy and distance to the Sink. Therefore, the route created by the protocol is secure against malicious attacks and is globally optimized according to the relevant information.

In WSN, it is relatively easy for sensor nodes (SNs) to be captured by attackers, then act as malicious nodes that launch various attacks, such as selective forwarding, wormholes, sinkholes, hello flooding and Sybil. To ensure secure routing and reduce energy consumption of SNs in WSNs, we also propose to use APs to represent the reliability of each SN. Accordingly, we select one SN at a time to improve the data communication success rate without determining the type of attack, along with identifying the SN with more residual energy and closer to the Sink which will be selected as the next forward node. As such, a balance between security and power consumption can be achieved for each SN.

Regarding the system model, we assume that a WSN consists of *n* nodes and use the network topology as its topology. $G = (V, E, W)$, $V = N \cup \{\text{Sink}\}$, N represents the set of SNs, E represents the set of connected edges SNs and $W = \{w_{ij}/(v_i, v_j)$ is an edge of $E\}$ and is also the set of weights associated with the edges. *G* has a single Source Sensor Node (SSN) and a Sink. For any two nodes *s* and *d* of *V*, the transmission path $\langle m_1, \ldots, m_{K+1}\rangle$ of length K is the K-hop path between them, where $m_1 = s$, $m_{K+1} = d$ and $\langle m_1, m_{K+1}\rangle$ is an edge of E, $\forall I \in \{1, \ldots, K\}$. Therefore, a path from SSN to Sink in *G* can be written as $l_s = \langle SSN, Sink\rangle$. Along with a multi-hop path to the Sink, data can be transmitted to the Destination Sensor Node (DSN). However, when there are malicious nodes (that is, some of G's nodes are occupied by the attacker and act as malicious nodes), the *K*-hop path $\langle m_1, \ldots, m_{K+1}\rangle$ can not guarantee successful data transmission between m_1 and m_{K+1}.

In our approach, a node captured by an attacker becomes a malicious node that initiates an internal attack on other nodes and we also view this attack as a model of the attack. selective forwarding. Also, in this approach, the trust value of a node is evaluated according to its history of normal and anomalous communication behaviors. At the same time, SSNs are divided into four categories: normal SSN, malicious SSN, faulty SSN and dead SSN. However, for the sake of simplification, we consider both failed and dead nodes as malicious nodes because all three types have significantly increased packet loss rates.

Malicious nodes in the WSN can initiate internal attacks, so it is necessary to find a secure route to ensure successful data transmission. We use *AP* to evaluate the reliability of the route between two nodes. To find the optimal relay node for a given node i, it is necessary to compute the *AP* of the nodes adjacent to it. Fig. 5 and Fig. 6 show the AP calculation method. For the adjacent node *j* of *i*, the previous communication behavior between them will be used to compute the *AP*. The $AP_{(i,j)}$ attack probability of *j* to *i* consists of two parts: (1) direct attack probability $AP_{d(i,j)}$ and (2) indirect attack probability $AP_{ind(i,j)}$.

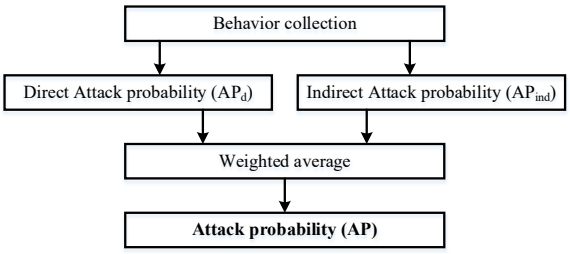

Fig. 5. Calculation process of the attack probability

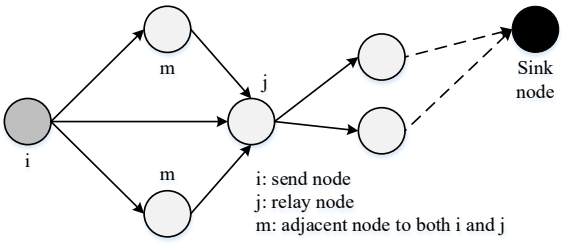

Fig. 6. Direct or indirect attack probability

Equation (1) shows a method for calculating the direct *AP* of j according to its previous communication behaviors with i.

$$AP_{d(i,j)} = \frac{|P_{ij} - P_j|}{P_{ij}} \quad (1)$$

where P_{ij} is the number of packets sent from i to *j* and P_j is the number of packets successfully forwarded by node j in the past. Direct *AP* is defined as the packet loss rate of node j, i.e. the ratio between the number of packets lost and the number of packets sent to *j* from *i*.

The indirect *AP*, as shown in *cn (2),* calculates the attack probability of *j* according to previous communication behaviors with nodes adjacent to both *i* and *j*.

$$AP_{ind(i,j)} = \frac{\sum_{m=1}^{\gamma} \alpha_m AP_{d(m,j)}}{\sum_{m=1}^{\gamma} \alpha_m} \quad (2)$$

$$\left(\alpha_m = 1 - AP_{d(m,j)}, m \neq i\right)$$

where *m* is the node adjacent to both i and j, α_m is the confidence value of node *m* from *i* and *r* is the number of nodes adjacent to both *i* and *j*. The indirect *AP* of

node *j* is determined by the *AP* of *j* to *m*. It is the weighted average of the direct *AP* of *j* to all nodes adjacent to both *i* and *j*. In this way, even if some nodes intentionally reduce the malicious node's *AP* by transmitting an error value, the malicious node's *AP* can be calculated by other nodes. Therefore, the bug has little effect on the overall *AP* and can be resistant to collusion attacks.

Combining (1) and (2), we have the *AP* of node *j*, like (3)

$$AP_{i,j} = \frac{\sum_{m=1}^{\gamma} \alpha_m AP_{d(m,j)}}{\sum_{m=1}^{\gamma} \alpha_m} \quad (3)$$

$$\left(\alpha_m = \begin{cases} 1, & m = i \\ 1 - AP_{d(m,j)}, & m \neq i \end{cases}\right)$$

According to [15], a WSN is very similar to a serial parallel system in classical reliability theory. A route between two nodes in a WSN can be thought of as a serial system and a WSN can be seen as a complex parallel system because there is more than one route per pair of nodes. Data can be transmitted along parallel routes and can only be successfully transmitted to a sink node along a particular route if all nodes in the route are working properly. Thus, the nodes in a route can be viewed as a serial system of independent components. According to serial system theory, the *AP* of a path *(l* = $\langle m_1, \dots, m_{K+1} \rangle$*)* can be calculated as

$$AP_L = 1 - \prod_{k=1}^{K} \left(1 - AP_{(m_k, m_{k+1})}\right) \quad (4)$$

where *K* is the number of hops. In the WSN, the state of each node *j* is associated with two values: (1) Residual energy and (2) its distance from the sink node. The state of each node is used as an experience to find the optimal safe route. A node with more residual energy closer to the sink node is selected as the next hop node. To balance power consumption and transmission delay for a sensor node, the state value for each node is determined by

$$E_j = \frac{\eta e_{(j,sink)}}{\eta e_{(j,sink)} + e_{rj}} \quad (5)$$

where $e_{(j,sink)}$ is the energy required to send a packet from *j* to the Sink, and e_{rj} is the residual energy of node *j*. We use the constant h to balance the weights of $e_{(j,sink)}$ and e_{rj}. With equation (5), it is possible to designate a node as the next hop if it has more residual energy and is closer to the sink node. We further define the E_L value for the whole path

$$E_L = \sum_{k=1}^{K} \left(\frac{\eta e_{(m_{k+1},sink)}}{\eta e_{(m_{k+1},sink)} + e_{rm_{k+1}}} \times \frac{1}{K} \right) \quad (6)$$

The E_L value of the entire path is obtained by adding the state values of each node. E_L is normalized to ensure that it is always less than 1.

Each node in the WSN is associated with information such as trust value (probability of an attack) and state (residual energy and distance to the sink). We use *AP* to represent a node's trust value and the power consumption required to send packets from a node to the Sink to reflect the distance from the node to the Sink. From the collected node information, the current and future trust values as well as the state of each neighboring node are sensed by the proposed cost function. Thus, the minimal cost forwarding node will be found. The cost function for a node takes up three aspects: (1) the *AP* for the path from itself to the sink, (2) the remaining energy of each node in the path, and (3) the distance from each node in the incoming path Sinks.

When a node n senses the data and transmits the data to the Sink, it selects a relay node s_n from its neighbors and then forms a *K*-hop link $ln = \langle m_1, \dots, m_{K+1} \rangle$ to the Sink in the rotation. The cost function of node n consists of two parts, $c_{n(1)}$ and $c_{n(2)}$, which are calculated for the *AP* and state values of the nodes in the path, respectively.

$$c_{n_{(1)}} = A_L = 1 - \prod_{k=1}^{K} \left(1 - AP_{\langle m_k, m_{k+1} \rangle}\right)$$

$$= AP_{\langle n,S_n \rangle} - \left(1 - AP_{\langle n,S_n \rangle}\right) \left[1 - \prod_{k=2}^{K} \left(1 - AP_{\langle m_k, m_{k+1} \rangle}\right)\right]$$

$$= AP_{\langle n,S_n \rangle} - \left(AP_{\langle n,S_n \rangle} - 1\right) c_{S_n(1)} \quad (7)$$

$$c_{n_{(2)}} = E_L = \sum_{K=1}^{K} \left(\frac{\eta e_{\langle m_{k+1},sink \rangle}}{\eta e_{\langle m_{k+1},sink \rangle} + e_{rm_{k+1}}} \times \frac{1}{K} \right)$$

$$= \left(\frac{\eta e_{\langle S_n,sink \rangle}}{\eta e_{\langle S_n,sink \rangle} + e_{rS_n}} \times \frac{1}{K} \right) + \sum_{k=2}^{K} \left(\frac{\eta e_{\langle m_{k+1},sink \rangle}}{\eta e_{\langle m_{k+1},sink \rangle} + e_{rm_{k+1}}} \times \frac{1}{K} \right)$$

$$= \left(\frac{\eta e_{\langle S_n,sink \rangle}}{\eta e_{\langle S_n,sink \rangle} + e_{rS_n}} \times \frac{1}{K} \right) + c_{S_n(2)} \quad (8)$$

The cost function of *n* is

$$c_n = c_{n(1)} + c_{n(2)} \quad (9)$$

Equations (7) - (9) show that the cost of a node *n* is determined by the quality of the current hop on the path and that the cost of a neighbor *sn* is chosen by *n*; therefore, global optimization can be guaranteed.

6. Conclusion

In this paper, we have investigated different secure routing protocol classification methods in WSNs [1, 3], [11-14], which propose a general classification of secure routing protocols.

The main challenge for secure routing protocols in WSNs is the limited power resources of wireless sensor nodes. However, these wireless sensor nodes work mainly to transmit and receive data, so it will consume a lot of energy. Therefore, the secure routing protocols need to ensure the most energy efficiency so

that the wireless sensor nodes operate for as long as possible to prolong the life of the WSNs.

When a wireless sensor node becomes inactive due to a lack of power or failure, the remaining wireless sensor nodes will increase communication energy consumption. Therefore, the important goal of secure routing protocols is to maintain network connectivity to perform routing and prolong the lifetime of WSNs.

On the other hand, congestion in WSNs not only impedes data transmission but also causes packet loss and thus packet retransmission requirements leading to power depletion of wireless sensor nodes. Therefore, the congestion avoidance method is used to prevent the occurrence of congestion and the congestion control method is to eliminate the existing congestion.

Furthermore, WSNs are required to ensure confidentiality, authentication, integrity, availability, and novelty to prevent potential attack patterns. Therefore, it is necessary to study specific security requirements.

References

1. Christos Nakas, *et al.*, Energy efficient routing in wireless sensor networks: a comprehensive survey, Algorithms 2020, 13, 72; https://doi.org/10.3390/a13030072
2. O. A. Khashan, Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment, IEEE Access 8 (2020) 66878-66887. https://doi.org/10.1109/ACCESS.2020.2984317
3. Vivek Sharma and Devershi Pallavi Bhatt, A review on recent trends in secure and energy efficient routing approach in wireless sensor networks, IOP Conf. Series: Materials Science and Engineering, ASCI-2020, 1099 (2021). https://doi.org/10.1088/1757-899X/1099/1/012044
4. H. Luo, Y. Lin, and S. K. Das, Routing correlated data in wireless sensor networks: a survey, IEEE Network, vol. 21, no.6, Nov/Dec. 2007, pp. 40-47. https://doi.org/10.1109/MNET.2007.4395109
5. Tripathi, A.; Gupta, H. P.; Dutta, T.; Mishra, R.; Shukla, K.K.; Jit, S. Coverage and connectivity in WSNs: a survey, research issues, and challenges. IEEE Access 2018, 6, 26971-26992. https://doi.org/10.1109/ACCESS.2018.2833632
6. Zhu, C.; Zheng, C.; Shu, L.; Han, G. A survey on coverage and connectivity issues in wireless sensor networks. J. Netw. Comput. Appl. 2012, 35, 619-632. https://doi.org/10.1016/j.jnca.2011.11.016
7. Ploumis, S. E.; Sgora, A.; Kandris, D.; Vergados, D.D. Congestion avoidance in wireless sensor networks: a survey. In Proceedings of the 2012 IEEE Panhellenic Conference on Informatics (PCI 2012), Piraeus, Greece, 5-7 October 2012; pp. 234-239 https://doi.org/10.1109/PCi.2012.83
8. Kavitha, T.; Sridharan, D., Security vulnerabilities in wireless sensor networks: a survey. J. Inf. Assur. Secur. 2010, 5, 31-44
9. Uthra, R.A.; Raja, S.V., QoS routing in wireless sensor networks - A survey, ACM Computing Surveys, Volume 45 Issue 1, 2012. https://doi.org/10.1145/2379776.2379785
10. Kandris, D, A hybrid scheme for video transmission over wireless multimedia sensor networks. In Proceedings of the IEEE 17th Mediterranean Conference on Control and Automation, Thessaloniki, Greece, 24-26 June 2009; pp. 964-969 https://doi.org/10.1109/MED.2009.5164670
11. Shio Kumar Singh, Routing protocols in wireless sensor networks - a survey, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010, pp. 63-83 https://doi.org/10.5121/ijcses.2010.1206
12. Vikas Bhandary, Routing in wireless multimedia sensor networks: a survey of existing protocols and open research issues, Hindawi Publishing Corporation Journal of Engineering, Volume 2016, https://doi.org/10.1155/2016/9608757
13. Yasir Arfat, Riaz Ahmed Shaikh, A survey on secure routing protocols in wireless sensor networks, I.J. Wireless, and Microwave Technologies, 2016, 3, 9-19 https://doi.org/10.5815/ijwmt.2016.03.02
14. Bharat Bhushan and G. Sahoo, Chapter 10 - Routing protocols in wireless sensor networks, Computational Intelligence in Sensor Networks, part of Springer Nature 2019, pp. 215-248. https://doi.org/10.1007/978-3-662-57277-1_10
15. Qiong Shi, Li Qin, Yinghua Ding, Boli Xie, Jiajie Zheng and Lipeng Song, Information-aware secure routing in wireless sensor networks, Sensors 2020, 20, 165, MDPI https://doi.org/10.3390/s20010165