Metric Properties of Building a List of Trusted Nodes during Selection of Data Transfer Routes in Wireless Sensor Networks

Boris Sovetov[1][0000−0003−3116−8810] and Tatiana Tatarnikova[2][0000−0002−6419−0072]

[1] Saint Petersburg Electrotechnical University "LETI", ul. Professora Popova 5, 197376 St. Petersburg, Russia
bysovetov@mail.ru

[2] Russian State Hydrometeorological University, ul. Voronezhskaya, 79, 192007 St. Petersburg, Russia
tm-tatarn@yandex.ru

Abstract. Known attacks aimed at routing a wireless sensor network are considered. An algorithm is proposed for generating a list of trusted nodes involved in the construction of logical data transfer routes between the sensor device and the nearest base station. The algorithm works independently on each head node of the clusters that make up the wireless sensor network. Mandatory and selective metrics that are involved in determining the list of trusted nodes are proposed. The simulation of a wireless sensor network consisting of the same sensor nodes and a base station located on the territory of a given size is performed. The model provides for the possibility of mobility (movement) of nodes and self-organization of the network. As a result of the model's work, text log files are generated that contain a list of events that occurred in the network — the appearance of data, the transfer of data packets, the exchange of reputation between nodes, as well as the network's functioning characteristics — the life cycle of the wireless sensor network and the percentage of lost packets. The results of a simulation experiment for a wireless sensor network with and without malicious nodes are presented, which showed the advantage of the proposed method of protection against routing attacks in terms of network operation characteristics.

Keywords: Wireless Sensor Network · Routing Attacks · Metric Characteristics · Node Reputation · Node Trust · Network Life Cycle · Malicious Node.

1 Introduction

Wireless sensor networks (WSN) are considered one of the most promising information and communication technologies of the 21st century. Inexpensive

and “smart” sensors integrated into a wireless network connected to the Internet provide a wide range of services for monitoring and controlling bodies, houses, enterprises, cars, etc. [1].

An important component of the installation and use of WSN is to ensure the information security of the transmitted data. WSNs are particularly vulnerable to routing attacks due to self-organization and limited resources of sensor nodes.

A self-organizing wireless network does not have a specific structure, and the functions of the nodes are not fixed. Each time a new device is connected to the network, the functions are redistributed between the network nodes and the characteristics of the communication channels change. This feature contributes to the development of attacks aimed at compromising the WSN nodes.

The limited resources of WSN sensor nodes, such as a small amount of computing power and memory, and battery energy reserve, contribute to the development of attacks aimed at shortening the WSN life cycle [2].

The lifetime of the WSN depends on the energy consumption of the sensor devices [3]. For this reason, methods of transmitting data to the WSN are aimed at reducing the number of operations performed by nodes. Energy consumption occurs during data transmission, processing, calculation of the route, etc. In connection with this, a common option is the hierarchical structure of building the WSN in which multi-step interaction is realized (Fig. 1) [4].

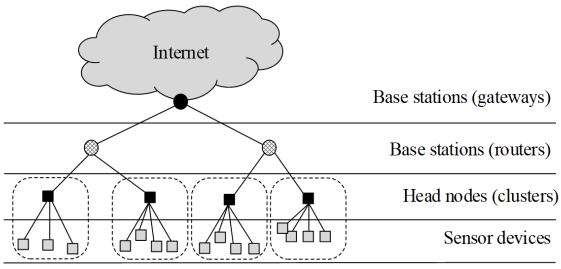

Fig. 1. Hierarchical structure of a WSN

Lower-level sensor devices first transmit data to the head nodes around which the devices are clustered. The head node is a sensory device that for some time performs the functions of a hub. These features include data aggregation, packetization of the sensor network, and relay to the nearest router. Routers form a mesh network topology through which packets are transported.

After several hops (jumps) data will be transmitted to the gateway – the output of the sensor network to the global network.

The time diagram of the life cycle of a clustered WSN is shown in Fig. 2.

The head node can be selected in the process of self-organization by chance or predetermined [5]. In the first case, each sensor device can become the head node with an equal chance, in the second case the head node is assigned based

on the central characteristics of the location of the sensor device in Euclidean distance or residual energy. The following head node selection algorithms can be used: LEACH, TEEN, PEGASIS and their subsequent modifications. A random selection of head nodes is preferable, since this allows you to create clusters of various sizes [6].

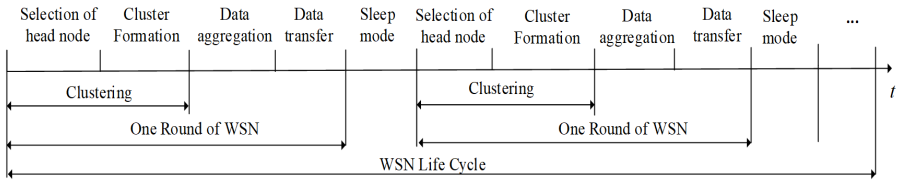

Fig. 2. WSN Life Cycle Diagram

2 Attacks aimed at routing in the WSN traffic

Consider known attacks aimed at routing in the WSN.

Wormhole attacks – its implementation requires at least two compromised nodes in different parts of the network. Packets intercepted on one compromised node Si are transmitted to another compromised node S_j outside the channel band. All nodes receiving a packet passing through the "wormhole" of node S_j will consider node S_i as their neighbor. Thus, with further data transfer, the routes will be built incorrectly. A wormhole attack is considered difficult to detect.

Assembly point attack – compromised node reports incorrect information about itself, for example, about a high energy reserve of the battery, thereby forcing neighboring nodes to refer to themselves as to the head node of a cluster.

Packet ejection attacks – there are two types of this attack: "black hole" and "gray hole". In a black hole attack, a compromised node destroys all received data. In the "gray hole" attack, packets are discarded selectively, which complicates its detection. These attacks are especially effective if the attacking node is the main one in the cluster.

Sibyl attack – a compromised node appears to other WSN nodes as multiple virtual nodes. When transmitting data through virtual nodes, the throughput of the WSN is significantly reduced.

Loop attack – using the features of the routing protocol, several compromised nodes can create a loop in the route, which leads to reduced bandwidth, data loss and increased power consumption.

Rush attack – lies in the propagation of service messages used in routing, which creates a decrease in throughput and, as a result, a reduction in the life cycle of the WSN.

3 Description of the proposed solution

The proposed solution is an algorithm for compiling a list of trusted nodes that can participate in the construction of logical data transfer routes from sensor devices to the nearest base station [8]. The algorithm works independently on each head node and consists of the following steps:

1. Initialization – each node determines its neighbors – nodes located at the distance of one hop and adds them to the list of trusted nodes. Initialization is performed once at the beginning of the deployment of the WSN.

2. Control – each node evaluates the behavior of its neighbors according to special metrics, according to which it determines its level of trust in them. The intrinsic trust of the node p to the neighbor node q is estimated as

$$C_{p,q} = \sum_{i=0}^{n} m_i w_i, \tag{1}$$

where $C_{p,q}$ is the level of trust the node p to the node q;
n is the quantity of metrics;
m_i is the value of the i-th metric;
w_i is the weight of the i-th metric.

3. Estimation of the reputation the neighboring node. The reputation of the node p to the node q is calculated as

$$R_{p,q} = \frac{\sum_{i=1}^{L} C_{p,i} C_{i,q}}{\sum_{i=1}^{L} C_{p,i}} \tag{2}$$

where L is the list of nodes exchanging trust.

4. Comprehensive estimation of the trust of the node to its neighbors based on their own trust and reputation gained from a third party. The confidence of the node p to the neighboring node q is estimated as

$$D = C_{p,q} \frac{z}{r} + R_{p,q} \left(1 - \frac{z}{r}\right) \tag{3}$$

where r is the quantity of interactions with the node;
z is the quantity of reputation exchanges with a node.

5. The node p makes a decision on interaction with the neighboring node q according to a logical rule: $D > P$?, where P is the limit level of trust.

6. The creation of the list of trusted nodes. Node p makes a decision about addition / exclusion of a node q to its list of trusted nodes.

The list of trusted nodes will be considered as a list of available nodes for further operation of the routing protocol.

4 Metrics Used

The metrics involved in determining the list of trusted sites are given in Table 1.

Table 1. Mandatory and selective metrics to define a list of trusted sites.

№	Metric Name	Estimation
	Necessary metrics	
1	The intensity of the packets	$m_1 = 1/N$, where N is the number of packets transmitted by the node in one round
2	The share of relayed packets	$m_2 = r^*/r$, where r^* is the number of packets transmitted through the node in one round; r is the number of interactions with a node in one round.
3	The proportion of correctly relayed packets	$m_3 = r^{**}/r^*$, where r^{**} is the number of packets correctly relayed through the node in one round;
4	The reputation exchange	$m_4 = z/r$, where z is the number of exchanges of reputation with a node in one round
5	The correctness of the reputation exchange	$m_5 = z^*/z$, where z^* is the number of correct reputation exchanges with the node in one round
6	The level of residual energy	$m_6 = E_j/E_0$, where E_j is the energy remaining on the j-th round of working WSN; E_0 is a node energy at the moment initialization WSN.
	Sample metrics	
7	Correctness reputation	$m_7 = \begin{cases} 1, \text{ if } C_{p,q} - \frac{\sum_{i=1}^{L} R_{i,q}}{L} \geq R_{\text{lim}} \\ 0, \text{ if } C_{p,q} - \frac{\sum_{i=1}^{L} R_{i,q}}{L} < R_{\text{lim}} \end{cases}$ where R_{lim} is the limit for the number of mismatches of trust levels with trust levels received from other nodes.
8	Historical trust	$m_8 = T(i-1)$, where $T(i-1)$ is the value of the level of trust to a node in the previous round of the working of the WSN.
9	Authentication	$m_9 = \begin{cases} 1, \text{ if the node has been authenticated,} \\ 0, \text{ if the node failed authentication.} \end{cases}$
10	Transmission Confirmation	$m_{10} = r^+/r^*$, where r^+ is the number of packets that received confirmation of their receipt for one round.
11	Data integrity	$m_{11} = \begin{cases} 1, \text{ if } CRC = CRC^* \\ 0, \text{ if } CRC \neq CRC^* \end{cases}$ where CRC is data field checksum written in packet format; CRC^* is checksum computed by the node based on the packet data field.

The list of metrics is not limited to those listed in Table 1. The contents of this list, as well as values of the weighting factors are determined by experts.

5 Wireless Network Model Description

The simulated network is a collection of 100 identical sensor nodes and a base station, located on an area of 200 to 200 meters in size. The nodes are randomly distributed over this territory and can move randomly in a radius of 2 meters in one iteration, if the protocol under study supports the mobility of the nodes. The range of the nodes is 25 meters.

WSN simulation model is created on the Java software platform. In the process of development, the principles of object-oriented programming were used, which made it possible to identify individual entities that describe the state and behavior of each of the WSN objects. List of the main programming interfaces that describe the components of the model:

Protocol – a software interface used to describe the clustering of the WSN and the initialization phase of the WSN.

Node – host. The touch node is characterized by the protocol with which it works, an identifier, a list of neighboring nodes, energy reserve, as well as other data used by the routing protocol, for example, the number of intermediate nodes to the base station. Also, an attacking effect on a network can be simulated on a node.

BaseStation – network gateway. Used to collect data from all network nodes. The gateway is located in the center of the sensor field, and unlike the WSN nodes, it has an unlimited supply of energy and cannot be attacked. Also, in the modeling process, the gateway is used to count correctly delivered packets.

Network – the entire sensor network, the totality of all nodes and the base station. It is used to create network components, initial placement of nodes, to simulate the appearance of data on nodes and to initialize attacking nodes. It is also used to collect data on the state of network nodes.

Attack – a software interface that describes the behavior of nodes simulating an attack.

TrustManager – software implementation of the proposed solution.

The software implementation of the model allows us to simulate the operation of the WSN with a different number of nodes and topologies. The network model allows you to use various protocols for routing, simulate attacks on the network by configuring nodes for attacking behavior. Also, the network model will allow a comparison of the network with nodes using the proposed solution to protect a network with the same network that does not use protection [7–10].

As a result of the program, text log files are generated containing a list of events that occurred in the WSN, for example, the appearance of data, the transfer of packets or the exchange of reputation between nodes. In addition, it is possible to add instructions that calculate other information about the network depending on the task, for example, the percentage of lost packets.

6 Experimental evaluation of the effectiveness of the developed solution on a software network model

To evaluate the effectiveness of the developed solution against energy depletion attacks, a comparison was made of the number of functioning nodes in the presence of a network of malicious nodes that depleted the energy of the WSN. The comparison was made between a network that does not use the proposed method of protection, a network without malicious nodes and a network that uses the proposed method. To assess the maximum possible efficiency of network protection, a network with malicious nodes was used as the upper boundary, but all malicious nodes were ignored by the network. In Fig. 3 shows the results of the experiment.

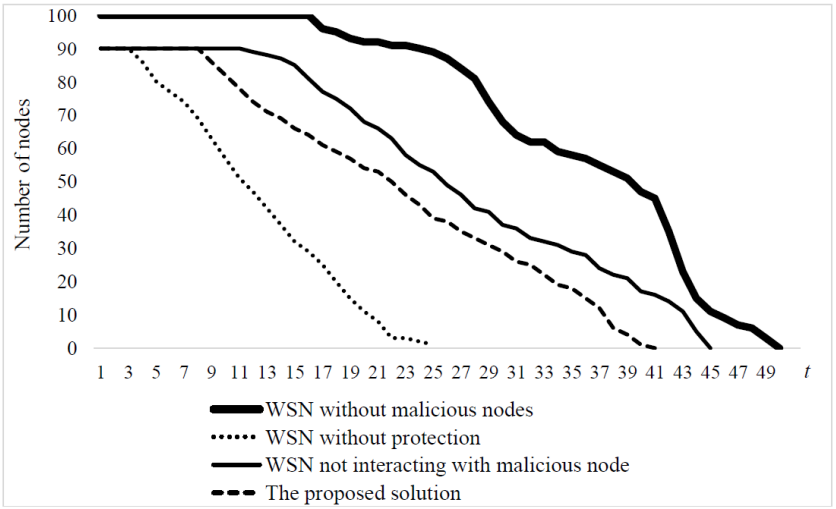

Fig. 3. Comparison of the life cycle duration of the WSN with malicious nodes

As can be seen from the graphs of Fig. 3, the proposed solution significantly increases the operating time of a network prone to energy depletion attacks. The difference from the upper boundary is due to the fact that the WSN nodes take time to collect statistics and detect malicious nodes. Metrics responsible for the transmission and integrity of data require additional energy costs.

An assessment was also made of the effectiveness of the proposed solution from the release or damage of data packets. A comparison was made of the number of lost or damaged packets between the network that uses the proposed solution and the network without protection, depending on the number of malicious nodes that damage data packets or attack a black and gray hole. In Fig. 4 shows the results of comparison.

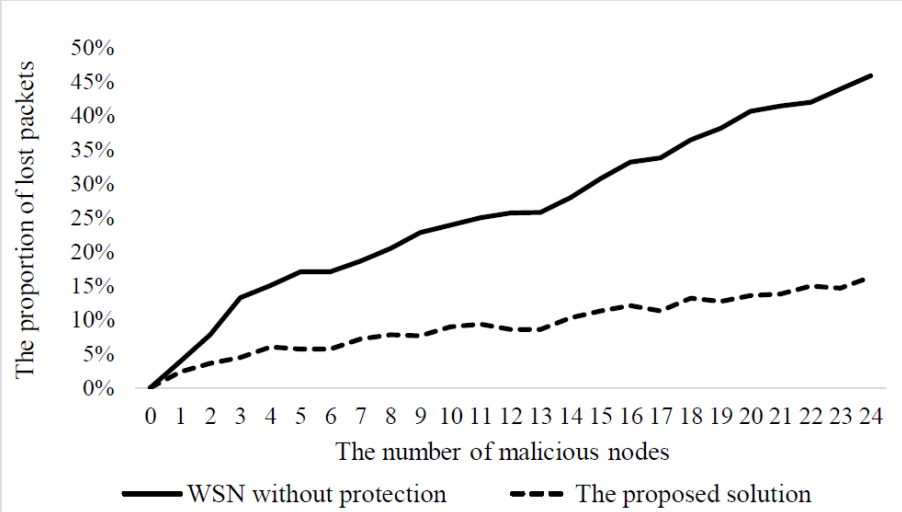

Fig. 4. Proportion of lost data packets depending on the number of malicious nodes

A similar experiment was carried out for networks with random attacks carried out by malicious nodes. The results are shown in Fig. 5.

As can be seen from the graphs of Fig. 3–5, the proposed solution significantly reduces the proportion of lost packets in the presence of malicious nodes in the WSN. The nonzero proportion of lost packets when using protection is explained by the fact that the network needs time to detect malicious nodes.

Thus, it was experimentally shown that the proposed solution is able to effectively protect the network from various attacks, reducing the number of lost data packets and increasing the operating time of the WSN.

7 Conclusion

A wireless sensor network has a number of features compared to classic wired networks, namely decentralization, limited resources and features of physical access to nodes. Attacks using the features of the WSN and directed to the process of routing data packets can lead to denial of service for the WSN nodes and, as a result, a reduction of the WSN life cycle duration.

Various metrics obtained on the basis of statistics on the interaction of WSN nodes and proposed in the article can help to identify malicious nodes and reduce the negative impact of the attacks they implement.

The results of the simulation experiment for the WSN with and without malicious nodes showed the advantage of the proposed method of protection against routing attacks over the WSN life cycle and the percentage of lost data packets.

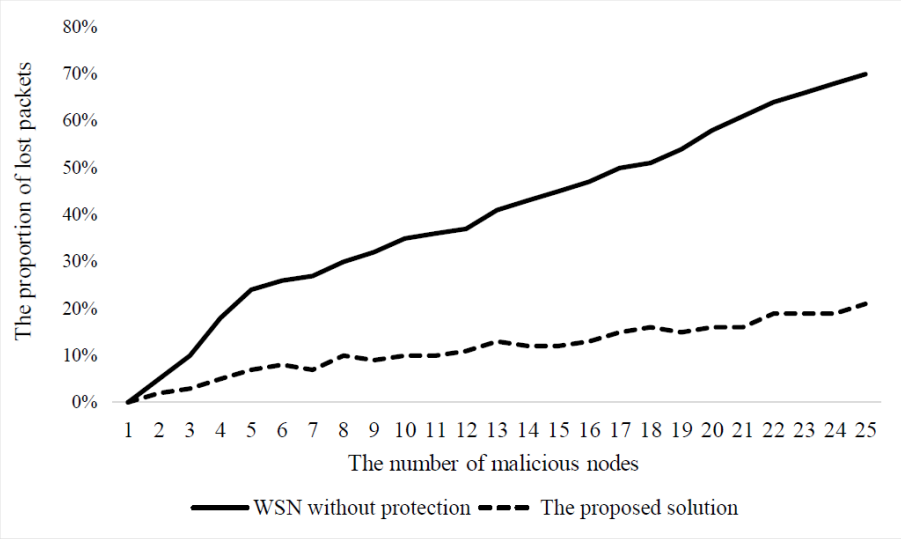

Fig. 5. Proportion of lost data packets depending on the number of malicious nodes (random attacks)

References

1. Doo-Soon Park. Fault Tolerance and Energy Consumption Scheme of a Wireless Sensor Network. In International Journal of Distributed Sensor Networks, vol. 3, 7 p. (2013). doi: 10.1155/2013/396850
2. Liu B. Dynamic Coverage of Mobile Sensor Networks / B. Liu, O. Dousse, Ph. Nain, D. Towsley // IEEE Trans. On Parallel and Distributed Systems, Feb. 2013. Vol. 24, № 2. P. 301–311.
3. Bonomi F. Fog computing and its role in the internet of things // Proceedings of the first edition of the MCC workshop on Mobile cloud computing, 2012. P. 13–16.
4. IEEE Std 802.11-2007, Revision of IEEE Std 802.11-1999. IEEE Standard for Information Technology-Telecommunications and information exchange between systems Local and metropolitan area network – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE Computer Society, June 2007.
5. Tatarnikova T. M., Dziubenko I. N. Wireless Sensor Network Clustering Model//2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2018. P. 1–4.
6. Hla Yin M., Win Z. Fault Management Using Cluster-Based Protocol in Wireless Sensor Networks // International Journal of Future Computer and Communication vol. 2, 2014. No. 6. P.36-39.
7. Bogatyrev, A.V., Bogatyrev, S.V., Bogatyrev, V.A.: Analysis of the Timeliness of Redundant Service in the System of the Parallel-Series Connection of Nodes with Unlimited Queues. In: 2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), (2018).
8. Dziubenko I. N., Tatarnikova T. M. Algorithm for Solving Optimal Sensor Devices Placement Problem in Areas with Natural Obstacles//2018 Wave Electronics and

its Application in Information and Telecommunication Systems (WECONF). 2018. P. 1–4. DOI: 10.1109/WECONF.2018.8604325
9. Bogatyrev V.A. Increasing the fault tolerance of a multi-trunk channel by means of inter-trunk packet forwarding (1999) Automatic Control and Computer Sciences, 33 (2) , pp. 70-76.
10. Tatarnikova, T.M. Statistical methods for studying network traffic. In Informatsionno-Upravliaiushchie Sistemy, vol. 96, no.5, pp. 35-43 (2018). doi: 10. 31799 / 1684-8853-2018-535-43