applied sciences

MDPI

Article

Utilising Acknowledge for the Trust in Wireless Sensor Networks

Hosam Alrahhal [1,2,*], Razan Jamous [1], Rabie Ramadan [3,4], Abdulaziz M. Alayba [3] and Kusum Yadav [3]

[1] Faculty of Engineering and Applied Science, University of Regina, Regina, SK S4S 0A2, Canada; razanadnanj@gmail.com
[2] Faculty of Engineering, Nahda University, Beni Suef 62764, Egypt
[3] College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia; rabie@rabieramadan.org (R.R.); a.alayba@uoh.edu.sa (A.M.A.); y.kusum@uoh.edu.sa (K.Y.)
[4] Computer Engineering Department, Faculty of Engineering, Cairo University, Cairo 12613, Egypt
* Correspondence: hosamrahhal@gmail.com

Abstract: Wireless Sensor Networks (WSNs) are emerging networks that are being utilized in a variety of applications, such as remote sensing images, military, healthcare, and traffic monitoring. Those critical applications require different levels of security; however, due to the limitation of the sensor networks, security is a challenge where traditional algorithms cannot be used. In addition, sensor networks are considered as the core of the Internet of Things (IoT) and smart cities, where security became one of the most significant problems with IoT and smart cities applications. Therefore, this paper proposes a novel and light trust algorithm to satisfy the security requirements of WSNs. It considers sensor nodes' limitations and cross-layer information for efficient secure routing in WSNs. It proposes a Tow-ACKs Trust (TAT) Routing protocol for secure routing in WSNs. TAT computes the trust values based on direct and indirect observation of the nodes. TAT uses the first-hand and second-hand information from the Data Link and the Transmission Control Protocol layers to modify the trust's value. The suggested TATs' protocols performance is compared to BTRM and Peertrust models in terms of malicious detection ratio, accuracy, average path length, and average energy consumption. The proposed algorithm is compared to BTRM and Peertrust models, the most recent algorithms that proved their efficiency in WSNs. The simulation results indicate that TAT is scalable and provides excellent performance over both BTRM and Peertrust models, even when the number of malicious nodes is high.

Keywords: wireless sensor networks; routing; trust; cross-layer; malicious

Citation: Alrahhal, H.; Jamous, R.; Ramadan, R.; Alayba, A.M.; Yadav, K. Utilising Acknowledge for the Trust in Wireless Sensor Networks. *Appl. Sci.* **2022**, *12*, 2045. https://doi.org/10.3390/app12042045

Academic Editor: Juan Francisco De Paz Santana

Received: 10 January 2022
Accepted: 14 February 2022
Published: 16 February 2022

1. Introduction

The standardization process for the Narrowband Internet of Things (NB-IoT) has been completed, and Wireless Sensor Networks (WSNs) are being considered as a critical component for sensing and collecting information [1]. WSNs are collections of hundreds of thousands of tiny devices with integrated sensing and wireless communication capabilities that are connected together, forming a wireless network. As a result of their limited or no mobility, they are considered a special case of ad hoc networks [2]. Several essential features of sensor networks are similar to those of Mobile Ad Hoc Networks (MANETs). For example, both require self-organization and wireless multihop operations, as well as time-variability in topology [3]. WSNs, which offer sensed information in context-aware and customized applications, have been extensively utilized in various areas, including intelligent connected vehicles, intelligent transportation, smart cities, precision agriculture, and environmental monitoring [4–6].

Because of the nature of the wireless medium, limited resources, and the sensors' natural cooperation, WSNs are vulnerable to several attacks (either self or malicious attacks,

i.e., misbehaving nodes). Customers do not want to share their information with unauthorized persons since the data may be misused. This additional consideration is of greater importance in wireless environments, because anybody may eavesdrop on unencrypted communication. For that, both external and interior security threats are significant threats to information security in WSNs. Creating a secure path in these networks must guarantee that all nodes used to send data packets are trusted nodes. Therefore, it is necessary to build an efficient trust model; where the node can evaluate the trustiness of all neighboring sensor nodes through the interaction between them.

The ability to make decisions in a WSN is critical for carrying out specific tasks since it assists sensors in forming collaborative efforts. It is thus necessary to implement a smart trust management scheme to determine the trustworthiness of sensor nodes, differentiate between malicious and good nodes, and boost trusted nodes while reducing the trust of suspicious nodes. Developing trust among sensor nodes has been identified as a new method to improve security in wireless sensor networks. Because sensor nodes have limited resources, especially battery power, the amount of energy used by sensor nodes is critical. Since these networks are designed to operate unattended in hostile environments for several years, energy replenishment is almost impossible under these conditions. One of the most challenging design concerns in WSNs is having limited energy resources, which implies that choosing sensor nodes for tasks should be done carefully to help keep WSNs alive.

The WSN might suffer from serious system performance reduction if an inappropriate node is selected as a routing node. As a result, selecting one or many appropriate nodes to act as cooperation partners for any node in a WSN is a difficult task. The overall system stability of WSNs may be enhanced by choosing the most suitable sensor node throughout the collaboration process. The contributions of this paper can be summarized as follows:

1. Designing a new trusted routing technique for WSNs that uses first-hand and second-hand information and the acknowledgments (ACKs) from the data link and end-to-end TCP layers.
2. The protocol is proposed to detect and isolate the malicious sensors to create a free-malicious- end-to-end route, increasing the network's throughput and decreasing the network's energy consumption.
3. The proposed protocol performance is evaluated using different numbers of malicious sensors in the network and different network densities.
4. The proposed protocol is compared with existing BTRM and Peertrust models.

To simplify reading the paper abbreviations, Table 1 summarizes all used terms.

Table 1. List of abbreviations.

Abbreviation	Definition
WSNs	Wireless Sensor Networks
IoT	Internet of Things
TAT	Tow-ACKs Trust
BTRM	Bio-inspired Trust and Reputation Model
NB-IoT	Narrowband Internet of Things
MANETs	Mobile Ad-hoc NETworks
ACKs	ACKnowledgments
DDTMB	data-driven trust mechanism based on blockchain
LEACH-TM	Trust Management-based and Low Energy Adaptive Clustering Hierarchy protocol
SD	Standard Deviation
MAC	Media Access Control
CORE	COllaborative REputation
CONFIDANT	Cooperation of Nodes- Fairness in Dynamic Adhoc NeTworks
RR	Route Request

Table 1. *Cont.*

Abbreviation	Definition
TTSN	Task-based Trust framework for Sensor Network.
P2P	Peer-to-Peer
ID	identifier
IOP	Information of Packet
TCP	Transmission Control Protocol
RREQ	Route REQuest
RREP	Route REPly
ACK_{DLL}	Data Link–Layer ACKnowledgement
ACK_{TCP}	TCP Layer ACKnowledgement
MEM	Malicious Exploration Message
MDM	Malicious Discovery Message
RTT	Round-Trip Time
TRMSim	Trust and Reputation Models Simulator
MDR	Malicious Detection Ratio
APL	Average Path Length
AEC	Average Energy Consumption
MTE	Multi-Threshold Energy

The paper is organized as follows: Section 2 summarizes the related work, while the problem definition is presented in Section 3. The proposed protocol is described in Section 4. The results are explained in Section 5, and the paper concludes in Section 6.

2. Related Work

This section is dedicated to the most relevant literature on the proposed approaches in this paper.

An innovative method, game-based trust, is proposed in [7], which utilizes game theory to synthesize direct and indirect trust for decision-making and improve networks' robustness and security. Game theory based on indirect information is used to calculate indirect trust value. The authors of [8] also propose a data-driven trust mechanism based on blockchain (DDTMB) technology, which is a decentralized and energy-efficient solution for detecting inside attacks in the Internet of Things (IoT) powered Sensor Networks. The DDTMB utilizes data collected from internet of things devices to demonstrate the resulting communication. Similarly, a trust management-based and energy-efficient hierarchical routing protocol were also suggested in [9]. To reduce node energy consumption, LEACH-TM restricted the cluster size. Numerous metrics were utilized, including the number of dynamic decision cluster head sensors, sensors residual energy, and the number of neighbors. Furthermore, the trust-management model was integrated into LEACH-TM to overcome internal threats. Moreover, in [10], the author suggested a trust method for dynamic optimization depending on the entropy technique. The entropy weight model chooses the sensor weights in every set. After that, the Standard Deviation (SD) value for local group evaluation is computed to obtain the general expectations of all sensors within the set, likewise the SD of Local Evaluation.

In [11], the authors presented a Time Series Trust method depending on the Toeplitz matrix and trust-based Auto-Regressive strategy. The effect of the suggested method on data forecasting the gathering and rebuilding of compressed sensing evaluated via many performance factors and various attack methods. Another proposal was stated by the authors in [12], where they proposed a protocol Layer trust-Based Intrusion Detection System to protect the WSN through discovering the threats at various layers. The sensor's trust value was determined using the variation of trust indicators for every layer considering the threats. Additionally, the authors consider the truthfulness of trust in the PHY, MAC, and network layers. Lastly, the total node's trust value is calculated via summation of the trust values for the three layers. Based on the sensor's trust value, it is considered a trusted or attacker. To evaluate the trust and reputation of sensors in wireless sensor networks, the

authors in [13] proposed an Exponential-based Trust and Reputation Evaluation System to monitor sensors' activities and assess sensors' trust and reputation. The exponential distribution was used to compute the allocation of the sensors' trust. The sensor's trust was applied to find trusted sensors to transfer data and decrease malicious threats in the network. Moreover, the entropy notion was applied to get the uncertainty values of the first-hand trust. The second-hand trust was proposed to support interaction information from non-neighing nodes when the suspicion of the first-hand trust is large enough. Moreover, the authors used the confidence factor to regulate the value of the sensor's trust to debilitate the hurtful impacts of the malicious sensors.

To enforce node cooperation in Mobile Ad hoc Networks, the authors of [14] have suggested the CORE (COllaborative REputation) method. This method is developed and modified over time as a result of direct observations and information given by other members of the sensing community. Nodes exclusively share information about their positive reputation with one another. Confirmation of Nodes-Fairness in Dynamic Ad-hoc NeTworks (CONFIDANT) [15] is a distributed, symmetric reputation technique that relies on first-hand observation and second-hand suggestions from non-neighboring sensors. S. Ganeriwal et al. [16] presented a reputation-based architecture for sensor networks. It employs a watchdog to build trust. However, the watchdog cannot capture every event due to its fault or network error.

M. Pushpalatha et al. [17] have developed a trust-based and energy-aware MANET routing model. Using the reliability parameter, the pathfinding process determines which node has the highest level of trust, and energy is used as a router. The node accepts a Route Request (RR) packet from the origin node if its trust value is high; else, the RR packet is ignored. As a result, by incorporating re-evaluation and reputation fading, the Bayesian approach-based model [18] may facilitate recovery while also preventing the sudden exploitation of a positive reputation that has been established over time. Aside from that, the authors of [19] have suggested a Hermes method, which is a conceptual framework for trust-building in the context of dependable packet delivery in the presence of potential hostile nodes. This method uses both first-hand and second-hand information to alter the values of trust. The authors of [20] offer another distributed trust-based architecture, along with the election method for the trustworthy cluster heads. Each node maintains a trust table for all of the nodes in its surroundings; the contents of this table are only transmitted to the cluster head upon request. To rank sensors through correlation using exploring Markov Chains in the WSN, the authors in [21] improved a scheme called SensorRank. A Trust Voting system was presented to discover incorrect node readings, and if the sensor is misbehaving, the sensor will not share in the voting. According to H. Chen et al. [22], reputation-based trust is derived from the concepts of probability, statistics, and mathematical analysis. As a new concept in trust, the authors propose that "certainty" can be adopted in building trust. WSNs, according to the authors, are not capable of making decisions based on the "trust" output of a single incident. A reputation space and trust spaces were used in WSNs, and they can define the transition from reputation space to trust space. Moreover, using a trust-based LEACH protocol to enable safe routing, the authors of [23] have suggested integrating a trust management module with a trust-based routing module. The trust management module is responsible for establishing trust relationships among nodes using innovative methods to increase building trust and offer efficient monitoring and trust exchange. A modified version of the trust-based routing protocol uses the same head-selection algorithm and working phases as the original protocol, making decisions based on trust. Several researchers, including [24], have suggested a multi-angle trust mechanism for nodes in Wireless Sensor Networks. Moreover, it considers the sensing data, communication trust, and node's energy when assessing the trust and communication. Moreover, to provide a trust framework in Wireless Sensor Networks, the authors of [25] have proposed the TTSN protocol. There are various trust rankings for each sensor based on the task. The proposed method employs a watchdog strategy to monitor the behavior throughout these sensors' various events and

broadcast their trust values. Furthermore, Xiong et al. [26] presented a trust framework that uses a consistent approach for determining trustworthiness in terms of interaction but uses a decentralized implementation of the model to facilitate a structured P2P network. Consequently, in [27], BTRM-WSN, a bio-inspired trust and reputation model for WSNs, is provided to maintain the most trusted route to the most reputable node in a WSN. This methodology is built on an ant colony's bio-inspired approach.

The authors of [28] have proposed an encryption and trust evaluation model based on a blockchain in which the identities of the Aggregator Nodes (ANs) and Sensor Nodes (SNs) are stored. The authentication of ANs and SNs is performed in public and private blockchains. The trust values of SNs are computed to eradicate the malicious nodes from the network. Secure routing in the network is performed considering residual energy and trust values of the SNs. Sahoo et al. [29] have presented a trust-based mechanism for enhanced security integrated with an energy utility and reusability model with software-defined networking (SDN) to maximize energy utilization. They presented a framework with SDN for the service station in a WSN.

In [30], the authors proposed a model for trust management in IoT devices and services based on the simple multi-attribute rating technique (SMART) and long short-term memory (LSTM) algorithm. The SMART is used to calculate the trust value, while LSTM is used to identify changes in the behavior based on the trust threshold.

A Temperature-Aware Trusted Routing Scheme (TTRS) is proposed in [31]. TTRS is a hybrid trust model and a multifactor, depending on the trust value of sensor nodes, remaining energy, hop count, and routing strategy. The multifactor strategy selects trustworthy nodes to forward data and reduce energy utilization due to secure shorter routing paths. TTRS incorporates an efficient multifactor hotspot node detection algorithm (HNDA), route discovery, and a route maintenance mechanism to detect malicious relay nodes for consistent data delivery in an unattended environment.

The authors of [32] have proposed a dynamic network security mechanism. Firstly, the direct trust value of the node is established based on its behavior in the regional information interaction. Then, the comprehensive trust value is calculated according to the trust recommendation value and energy evaluation value of other high-trust nodes. Finally, node reliability and management nodes are updated periodically. Malicious nodes are detected and isolated according to the credibility to ensure the network's dynamic, safe, and reliable operation. Sumalatha et al. [33] have proposed a cross-layer security-based fuzzy trust calculation mechanism (CLS-FTCM) and the least overhead monitoring for WSNs by means of memory and energy demands to detect the faults happening at various places at the same time. The fault monitoring system is carried out using an enhanced convolutional neural network (ECNN) classifier to identify malicious nodes on the network, and the confidential value is determined for the trust values.

The authors of [34] focused on designing an energy-efficient and secure routing protocol for smart building WSNs. The process in the proposed framework is carried out in two stages. The first stage is the design of the optimal routing protocol based on the grid-clustering approach. The second stage involves designing a trust model for secure data transmission using the two-fish algorithm. A grid organizer was selected based on the sailfish optimization algorithm in the grid-based model. Subsequently, a fuzzy expert system selects the relay node to reach the shortest path for data transmission.

The authors of [35] have presented a well-organized trust estimation-based routing scheme (ETERS) that consists multi-trust (communication trust, energy trust, data trust) approach to alleviate several internal attacks, such as badmouthing, Sybil, selective forwarding, on–off, black hole, and gray-hole attacks for clustered WSN. The proposed multi-trust approach is used to analyze the credibility of sensitive monitored data. A novel and efficient cluster head selection algorithm (ECHSA) is employed to improve the performance of the cluster head (CH) selection process in clustered WSN.

However, most current techniques are developed for MANETs and not WSNs. For example, establishing trust among entities that retain a pre-shared key or digital certificate

requires the help of a central trust authority. These trust models cannot be used in many applications, including military applications in which placing a central trust authority on the battlefield is infeasible. So far, up to our knowledge, no one computed or modified the trust values using the cross-layer concept. Moreover, current techniques operate at one energy level, i.e., sensors transmit and receive messages until they die.

3. Problem Definition

The network could be modeled as a set of static sensor nodes S are randomly deployed in a 2-D field F and a sink node sink(s). The field F is assumed to have Sm as a number of misbehaving sensors in WSN, and Pm P_m(equal to $SmS_m/S\frac{S_m}{S})\frac{S_m}{S}$ is the probability that the node is malicious. The deployed sensors are assumed to be homogeneous, considering their initial energy, sensing range, and communication range are the same. Therefore, the communication range (cs) is the same for all nodes. Some sensors are marked as the transmission source, while others act as intermediate nodes. Malicious sensors attempt to obstruct network performance, participating in route setup operations. All sensors are assumed to participate in the routing process, including packets forwarding in a bi-directional communication symmetry on every link between the sensors. In addition, the destination sensor is assumed reliable; moreover, any route in the network can have only one misbehaving sensor. Each node can detect its neighbors in its sensing range; moreover, the node can mark some control packets as high priority by setting the priority flag; besides, each node has a unique identifier (ID). Every sensor has a prevention list, including the misbehavior nodes, the trustworthy table holding the trustworthy value of nodes, which broadcast to neighbors, and the Information of Packet (IOP) table to save the information about the received and processed data of TCP acknowledgment packets. The routing table of each node will create a new entry to store the value of trustworthiness of other nodes. The following questions can summarize the problem:

1. What are the nodes that can be trusted?
2. How can the cross-layer concept be sued to specify an accurate trust threshold to differentiate between legitimate and malicious nodes?
3. Is it possible to detect and isolate the misbehaving sensors in the network?
4. Can we guarantee that nodes are transferring the data packets correctly?
5. To prolong the network lifetime, which nodes should be chosen as the next hop minimizing the overall network's energy consumption?
6. What arrangements can be made to evade link break so the malicious-free route can appropriately be selected?

4. The Proposed Technique

In this section, we describe the proposed protocol, the mathematical framework of the proposed protocol, and the pseudocode and flowchart for the proposed technique.

4.1. Description of the Proposed Technique

As described in the dictionary, the meaning of trust is "confidence in a person or thing's integrity, strength, ability, surety" [36]. Therefore, trust must be automatically adjusted, reflecting the dependability changes in others. This concept is applied to create a framework for sensors in WSNs to make correct decisions for path selection.

This paper presents a reactive trust-based routing method focusing on packet dropping attacks where misbehaving sensors try to reduce the network throughput. In this case, the malicious sensor transmits data link–layer acknowledgments (ACK_{DLL}) to neighbor sensors, thus delaying the discovery of the attack. This kind of attack is one of the worst attacks where it delays attack detection. The proposed technique consists of four phases: Initialization, Path Search, Data Transmission, and Paths Maintenance phases.

1. Initialization Phase

At the start of this phase, the sensors exchange the HELLO message with one another. A node receives a HELLO message for the first time, and it causes that node to update the information in its neighboring nodes table with this new information. As a result, at the end of the initialization process, every node will modify its adjacent node database.

2. Path Search Phase

When a source needs to transmit data packets to a destination and does not have a suitable path, the source starts the path search process to find a valid path. In this phase, the source sends a modified RREQ packet containing a list of ignored nodes that the source sensor wants to isolate from the discovered path temporarily. In addition, the destination sensor may have this list and discard all paths that contain these ignored nodes. Upon REQUEST reception, a relay node (i.e., an intermediate node) compares its current, trustworthy value of the previous node with this value contained in the RREQ packet. The relay node updates it as soon as a current value falls below the RREQ packet's value. When the destination sensor receives the RREQ packet from multiple nodes, it chooses two-node disjoint paths with the greatest trust value, and unicasts RREPs contain the trustworthy path value back to the source, including the selected two routing paths. The source selects the highest trusted path as the main used for data transmission and the second as an alternate path.

3. Data Transmission Phase

The source transmits its data packets over the main path, waiting to receive and in return from its downstream neighbor and from the destination over both primary and alternate paths, respectively. Each intermediary node stores its received information. If the source gets the ACK_{DLL} from its downstream neighbor as well as the through both the main and alternative routes, it positively updates the nodes' trust value and notifies the path nodes to update their trust value. If no is received through any of the routes, the source concludes that there is a misbehaving sensor in the routing paths and initiates the paths Maintenance Phase to identify and isolate any misbehaving sensors.

4. Paths Maintenance Phase

The source node sends a high-priority Malicious Exploration Message (MEM) containing information about the lost data packet to the destination node through the main path in the Paths Maintenance phase. Each node that gets the MEM has its data packet information recorded in its IOP table, compared to the MEM information. After finding a match, it will send the MEM to the next node with overhearing to ensure that the neighbor node also forwards the MEM to the appropriate node. The node that found the mismatch will cease transmitting the MEM and will issue a high priority Malicious Discovery Message (MDM). The format of this message, such as MDM (discovering node ID, discovered node ID), with overhearing in the opposite direction, will be sent to the discovered misbehaving sensor toward the source or destination node. The node that discovers that its downstream node does not send the MEM produces the MDM in the opposite direction of the detected misbehaving sensor toward the source or destination node. It is then sent to the source through the trusted route after the destination node has received the MDM. When an MDM is received, each node that receives it will adversely modify the trust value of the accused node; the detecting node will also add the found node ID to its ignored node list.

4.2. Mathematical Framework

Due to the broadcasting properties of the wireless networks, a node may collect data about the packet-forwarding behavior of its neighbors, snooping all received MAC layer frames and storing packet delivery statistics. Based on Bayesian statistics and Beta distribution, the trust value, t, and Treatment Ratio (r) value signed to a node can be defined as follows: let L indicate the total number of packets transmitted correctly. In addition,

let N indicate the total number of packets sent for transmitting by the sensor up to the present time.

$$t = \frac{L}{N}\ (1) \tag{1}$$

$$r = 1 - \frac{\sqrt{12\ L\ (N - L)}}{(N+1)N} \tag{2}$$

The Worthiness (W) value associated with a pair (t, c) is calculated by mapping the trust value, t, and the Treatment Ratio value, r, into a single value to facilitate trust-based decision-making [19].

$$W(t, r) = 1 - \frac{\sqrt{(t-1)^2 + c^2(r-1)^2}}{\sqrt{1+c^2}} \tag{3}$$

where c is a parameter that determines the relative importance of the trust value (t) vs. the Treatment Ratio value (r). The "default" value of worthiness is defined as:

$$W_{def} = W(0.5, 0) \tag{4}$$

W_{def} Value, in this case, is the worthiness value assigned to a node with trust and confidence values are t and r = 0, respectively; we consider this as the initial threshold for worthiness. The sensor is considered trustworthy when the worthiness of a sensor exceeds W_{def}; otherwise, the sensor is viewed as untrustworthy. The notion of worthiness is generalized to the notion of viewpoint (V), which incorporates worthiness values information from non-neighbors nodes. Let denotes the viewpoint that node (i) has for node (k). If i and k are neighbors, the viewpoint equals the worthiness value, $W_{i,k}$ that node (i) has for node (k). If nodes i and k are not neighbors, the viewpoint, $V_{i,k}$ is computed as follow (Figure 1):

$$W_{i,k} = W_{i,x1}.W_{x1,x2}.W_{x2,k} \tag{5}$$

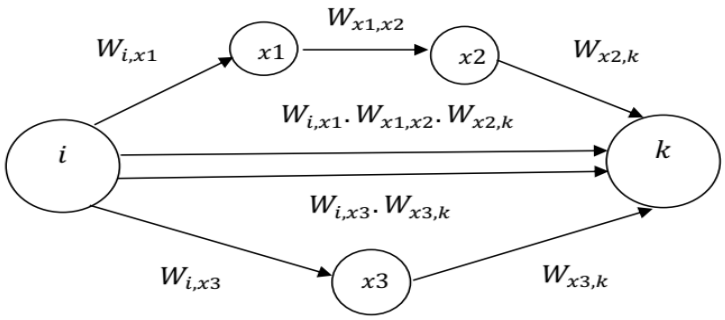

Figure 1. Example of viewpoint calculation for non-neighbors i and k.

Thus, the viewpoint can be defined as:

$$V_{lk} = \begin{cases} W_{ik} \text{ if i and k are neighbors,} \\ \max_{p \in P_{ik}} W_{ik}\ P_{ik} \neq \phi\ , \\ W_{def} \text{ otherwise,} \end{cases} \tag{6}$$

where P_{ik} is the set of paths between sensors i and k. $\overline{V}$ is the average of (V) over the watching windows.

To execute the routing decision, we may now apply a viewpoint metric to it or create a Multi-Trust level method, depending on the task's sensitivity to be executed to maintain a balance between traffic and energy in the WSNs. To compute the t, r, w, $\overline{V}$ values, two counters (L-counter, N-counter), and two timers are defined. In the first-timer, t_{DLL}^{ack}, the timeout interval is assigned a value that is greater than the maximum round-trip time (RTT) between two neighbor nodes. The second timer, t_{TCP}^{ack}, the timeout interval is set to a value based on the network diameter. To update L-counter and N-counter, the following approach is applied:

- When sensor (i) sends a packet (p) to node (j), the N-counter (i) is incremented by one, and the timers are initiated.
- If the acknowledgments from the data link layer (ACK_{DLL}), and TCP layer, (ACK_{TCP}), are received by node (i) before the timers expire, the L-counter (i) will be incremented by one; else, the L-counter (i) is not updated.

Moreover, the two counters for all sensors in the entire route will be updated in the same way. If the source does not receive any end-to-end (ACK_{TCP}), it concludes that there is a malicious node in the routing paths and starts to detect the malicious sensor by sending the information of a dropped packet to the destination. Each sensor along the route compares this information with its saved information until the misbehaving sensor is discovered and isolated. With the proposed technique, the source sensors will be able to select more trustworthy routes instead of merely shorter routes and isolate any misbehaving sensors in WSN.

4.3. Flowchart and Pseudocode for TAT

The following pseudocode explains the suggested Algorithm 1.

Algorithm 1: The proposed protocol

```
start
while (termination condition is not met) do
        if (No ACK_DLL) is received, then
        The link is excluded.
        else if (ACK_TCP) is received, then
                {
                  Compute credit value.
                  The sensors in the path are credited.
                }
         else
                 {
                    Compute penalty value.
                   The sensors in the path are penalized.
                 }
Take routing decision or multi-trust level application.
end- while;
end- algorithm
```

Figure 2 depicts a flowchart of the proposed routing protocol.

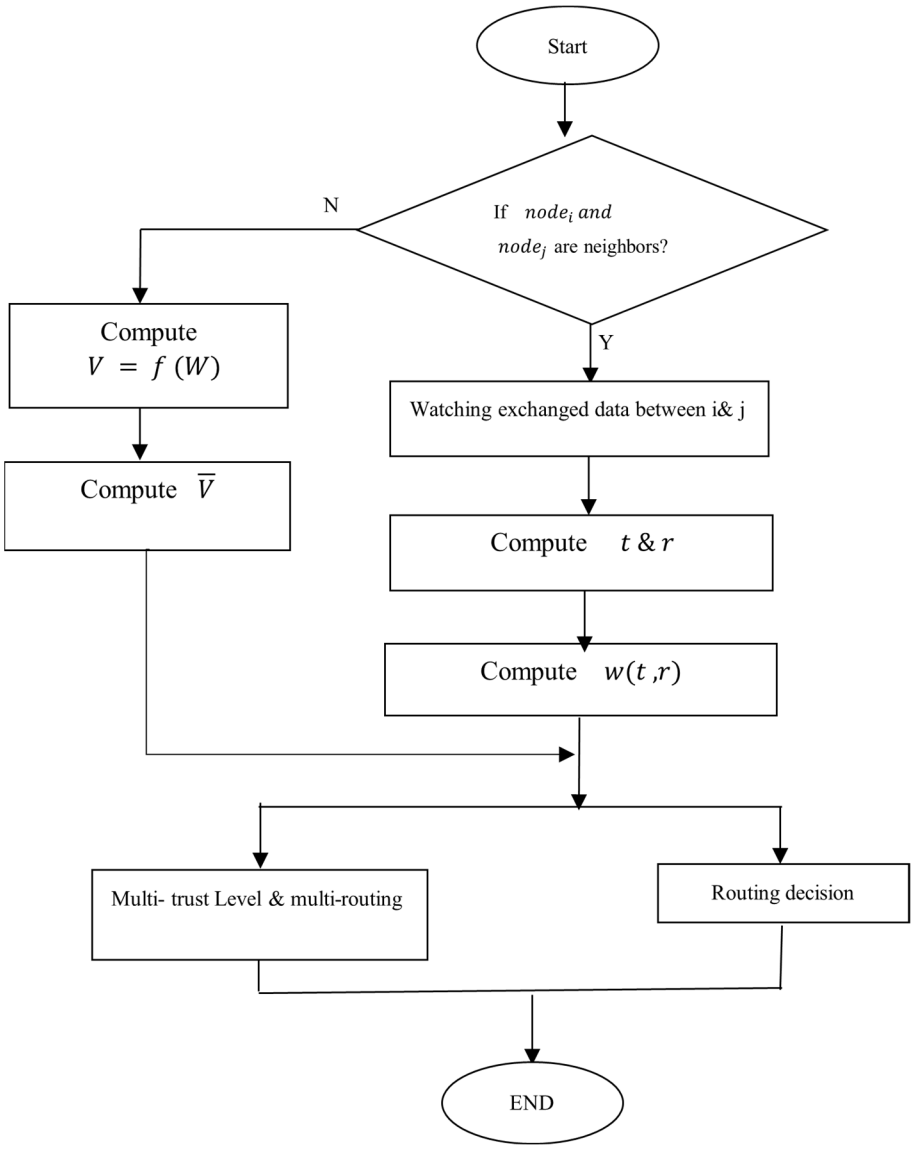

Figure 2. Flowchart of TAT Routing Protocol.

5. Results and Analysis

To assess the effectiveness of the suggested methods, we put our new model to the test against a number of random-topology WSNs using the TRMSIM-WSN simulator [37]. Some modifications have been made to satisfy the proposed approach requirements. Sensors are distributed in a (100 × 100) m^2 area, and each of them has a sensing domain of 10 m. We run the simulator under the same Configuration Parameters for all cases, networks' number = 50, the executions' number over each network = 100, i.e., every client requests service 100 times. Additionally, the proportion of the client is equal to 15 percent, the relay is equal to 10 percent, and malicious sensors range from 5 percent to 35 percent; the rest are benevolent sensors and the nodes' number (equal to 100 sensors) in each network. We will run the simulator for 300 s. For the purpose of evaluating the efficacy of the proposed model, we compute the following performance metrics:

1. Malicious Detection Ratio (MDR): The percentage of sensors in the WSN has been identified as misbehaving.
2. Accuracy Standard deviation (SD).
3. Average Path Length (APL) or the number of hops to trusted destinations.
4. Average Energy Consumption (AEC) (μJ): It measures the needed AEC of our proposed approach.

To evaluate the performance of the proposed model and verify its effectiveness, two simulations were conducted in two different scenarios:

(1) In the first scenario, we studied the impact of the network density on the performance of the proposed protocol. For that, the network size differs in Figures 3–5.
(2) In the second scenario, we compared the proposed protocol (TAT) with other protocols (BTRM and PeerTrust); thus, the network size is the same in Figures 6 and 7.

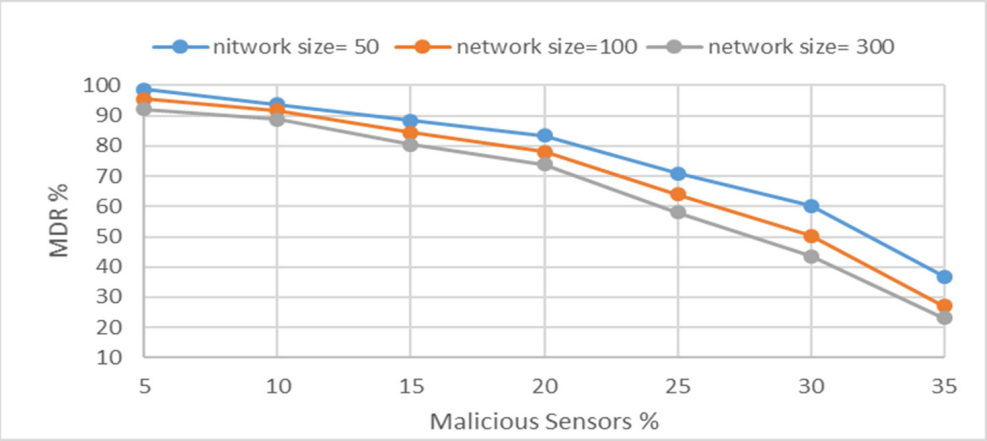

Figure 3. MDR vs. % malicious sensors in WSNs.

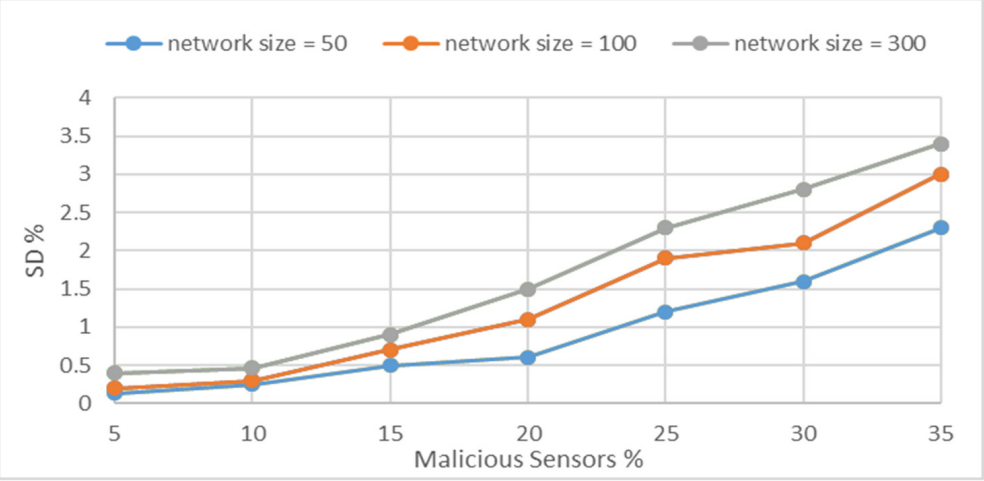

Figure 4. SD% vs. % malicious sensors in WSNs.

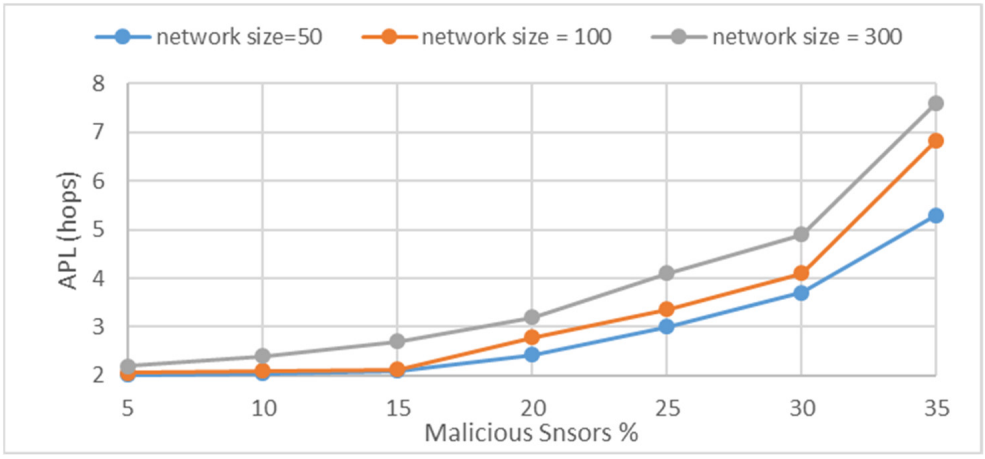

Figure 5. APL vs. % malicious sensors in WSNs.

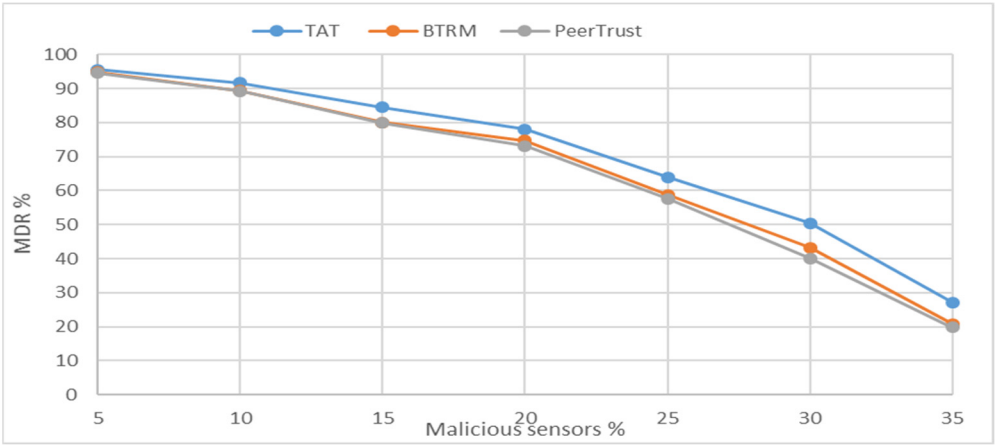

Figure 6. MDR for TAT, PeerTrust, and BTRM Models.

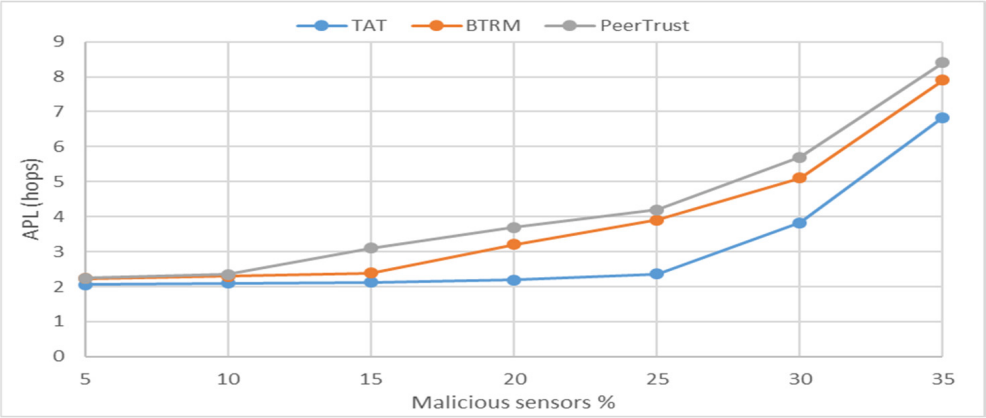

Figure 7. APL for TAT, PeerTrust, and BTRM Models.

First, we study the impact of the misbehaving sensors on the suggested technique, i.e., we evaluate the suggested technique when the percent of the misbehaving sensors increased in the static scenario. Then, we will compare the suggested model results with other existing models. Figure 3 shows the variation in MDR vs. the percent of misbehaving nodes in the WSN for different density values of the WSN.

As shown in Figure 3, it is demonstrated that when the MDR decreases, the number of misbehaving sensors increases. Moreover, the proposed model achieved MDR above

60% when the number of misbehaving nodes was not greater than 25%. Therefore, from Figure 3, we can deduce that the suggested method is scalable.

The variation in SD of MDR vs. the percent of misbehaving nodes in WSN is presented in Figure 4. In addition, as given in the figure, although the WSN size is 300 sensors, which is a large number of sensors, the standard deviation remains low (less than 3.5%). A shorter route towards trustworthy destinations entails less involved sensors; as a result, there is less global use of resources such as energy.

The variation in the APL vs. the percent of misbehaving nodes in WSN is presented in Figure 5.

For a given WSN, the APL increases with the percentage of malicious nodes increases. So the route to the server that has the service or destination will be longer, and APL will increase. As given, while the number of misbehaving nodes is not more than 25%, any trustworthy destination is never reached at more than four hops, on average.

Table 2 shows the AEC in the networks vs. the percentage of the misbehaving nodes in the WSN.

Table 2. Total AEC (μJ) in the network.

Malicious%	Network Size = 50	Network Size = 100	Network Size = 300
5	1.8×10^3	1.4×10^6	1.4×10^8
10	1.9×10^3	1.7×10^6	1.6×10^8
15	2.1×10^3	1.9×10^6	1.7×10^8
20	3.1×10^3	3.3×10^6	1.9×10^8
25	3.4×10^3	7.3×10^6	2.2×10^8
30	6.4×10^3	12.3×10^6	8.3×10^8
35	9.9×10^3	30×10^6	21×10^8

Two direct conclusions can be deduced from Table 2. Firstly, the higher the density of WSNs is, the higher the energy needs. However, as the number of misbehaving nodes increases, so does the power consumption. Due to the misbehaving nodes in a WSN that are a majority, it is harder to identify a trusted node, and as a result, more messages are transmitted. Therefore, to send out more messages, more energy is consumed.

The proposed TAT technique is compared with two existing models, PeerTrust [26] and BTRM [27]. Figure 6 shows the comparison between TAT, PeerTrust, and BTRM models regarding the Malicious Detection Ratio (MDR%).

From Figure 6, MDR's precision for all methods decreases as the percent of misbehaving sensors in the WSN increases because the percent of trusted sensors in the neighborhood for each node will decrease. Consequently, the precision of selection trustworthy next hop will decrease. Moreover, we can see that the performance of the proposed approach overcomes other models since we use monitoring tools at the link level (ACK_{DLL}) and for the entire path (ACK_{TCP}).

The result of a comparison between the proposed approach and other approaches according to the APL and the percent of malicious sensors in the network are shown in Figure 7.

The value of APL rises as the number of malicious sensors in the network grows, as shown in Figure 7. Consequently, the number of malicious sensors in the network is increasing, which means there will be fewer number of good nodes surrounding each sensor, reducing the chance of discovering to send to in the next hop. Moreover, it is clear that the value of the average path length for the proposed approach is better than other approaches, because the MDR of the proposed model is better than other models. Therefore, the number of trust neighbors will be higher; as a result, the probability of finding trust next hop is increased.

Table 3 shows the average values of total energy consumption for all approaches.

Table 3. Total AEC (μJ) in the network for TAT, PeerTrust, and BTRM Models.

Malicious%	AEC		
	Peertrust	**BTRM**	**TAT**
5	2.6×10^6	2.2×10^6	1.4×10^6
10	3.7×10^6	2.9×10^6	1.7×10^6
15	4.8×10^6	3.4×10^6	1.9×10^6
20	6.8×10^6	5.9×10^6	3.3×10^6
25	10.5×10^6	8.8×10^6	7.3×10^6
30	19.8×10^6	15.1×10^6	12.3×10^6
35	43.9×10^6	39.8×10^6	30×10^6

From Table 3, when the percentage of misbehaving nodes in a WSN increases, the energy consumption will increase. In other words, the broken links will increase. Additionally, more control packets must be generated, increasing energy consumption. Moreover, we can see that the suggested approach is more efficient in saving energy than other approaches since the MDR of the proposed approach is better than other approaches. In addition, the length of paths in the presented approach is shorter than other approaches; consequently, the consumption of energy will be decreased.

As a summary of the results, the proposed technique is able to detect and isolate the malicious sensors along the route from the source to the destination—therefore, creating a free-malicious- end-to-end route. Moreover, as can be seen, from the results, using the proposed technique, the malicious detection ratio (MDR) increases, and the Average Energy Consumption (AEC) decreases, expanding the network's throughput. In addition, A shorter route towards trustworthy destinations entails less involved sensors; as a result, there is less use of resources such as energy.

6. Conclusions and Future Work

Tow-ACKs Trust (TAT) Routing protocol is proposed to detect and isolate the malicious sensors to create a free-malicious- end-to-end route, increasing the network's throughput and decreasing the network's energy consumption. This paper suggests a new technique based on the cross-layer concept, TAT, which uses first-hand and second-hand information and the acknowledgments from data link and TCP layers to compute and update the trust values. The TAT performance was evaluated using different numbers of malicious sensors in the network and different network densities. In addition, we compared TAT protocol with existing protocols, namely PeerTrust, and BTRM. TAT increases the network expected lifetime and increases the malicious detection ratio packet delivery ratio, and decreases the energy consumption. The experimental results of evaluation TAT with different network sizes show that the proposed model is still efficient when the network size increases, which means TAT is scalable. Moreover, the results show that the proposed model showed better performance compared to PeerTrust, and BTRM models, in terms of Malicious Detection Ratio (MDR), Packet Delivery Ratio (PDR), and Average Energy Consumption (AEC), even with a high percent of malicious sensors. An analytical model for the proposed technique will be presented to extend the current work. Moreover, the proposed model will be examined against dynamic WSNs. Furthermore, the earlier Multi-Threshold Energy (MTE) technique [38] for the TAT method to minimize energy consumption can be applied for further performance enhancement. Moreover, End-to-End delay between trusted destinations could be used as a metric to evaluate the proposed technique in terms of time. Moreover, utilizing Artificial Intelligence (AI) techniques could be one of the valuable extensions to the work done in this paper, including artificial neural networks and particle swarm optimization with center of gravity (PSOCoG) [39] selecting the best settings values.

Author Contributions: H.A. and R.J. carried out conceptualization, methodology, software, and validation; H.A. and R.J. were responsible for formal analysis, data curation, writing, and the original draft preparation; H.A., R.J. and R.R. performed analysis, reviewing and editing. A.M.A. and K.Y. performed reviewing. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by the Scientific Research Deanship at the University of Ha'il—Saudi Arabia through project number BA-2101.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fang, W.; Zhang, W.; Chen, W.; Pan, T.; Ni, Y.; Yang, Y. Trust-based attack and defense in wireless sensor networks: A survey. *Wirel. Commun. Mob. Comput. J.* **2020**, *2020*, 2643546. [CrossRef]
2. Cordeiro, C.; Agrawal, D. *Ad Hoc & Sensor Networks: Theory and Applications*, 2nd ed.; World Scientific Publishing Company: London, UK, 2011; p. 664.
3. Willig, A. Wireless sensor networks: Concept, challenges and approaches. *Elektrotechnik Inf. J.* **2006**, *123*, 224–231. [CrossRef]
4. Li, J.; Cai, T.; Deng, K.; Wang, X.; Sellis, T.; Xia, F. Community-diversified influence maximization in social networks. *Inf. Syst. J.* **2020**, *92*, 101522. [CrossRef]
5. Cai, T.; Li, J.; Mian, A.S.; Li, R.; Sellis, T.; Yu, J.X. Target-aware holistic influence maximization in spatial social networks. *IEEE Trans. Knowl. Data Eng. J.* **2020**, *4347*, 1–14. [CrossRef]
6. Wang, X.; Ning, Z.; Zhou, M.; Hu, X.; Wang, L.; Zhang, Y.; Yu, F.R.; Hu, B. Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. *IEEE Commun. Surv. Tutor. J.* **2018**, *2018. 21*, 1314–1345. [CrossRef]
7. Yi, L.; Fang, W.; Zhang, W.; Gao, W.; Li, B. Game-Based Trust in Complex Networks: Past, Present, and Future. *Complex. J.* **2021**, *2021*, 6614941. [CrossRef]
8. Sivaganesan, D. A Data Driven Trust Mechanism Based on Block chain in IoT Sensor Networks for Detection and Mitigation of Attacks. *J. Trends Comput. Sci. Smart Technol.* **2021**, *3*, 59–69. [CrossRef]
9. Fang, W.; Zhang, W.; Yang, W.; Li, Z.; Gao, W.; Yang, Y. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digit. Commun. Netw. J.* **2021**, *7*, 470–478. [CrossRef]
10. Nie, S. A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. *Clust. Comput. J.* **2019**, *22* (Suppl. 5), 11153–11162. [CrossRef]
11. Gilbert, E.P.K.; Kaliaperumal, B.; Rajsingh, E.B.; Lydia, M. Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks. *Comput. Electr. Eng. J.* **2018**, *72*, 894–909. [CrossRef]
12. Ghugar, U.; Pradhan, J.; Bhoi, S.K.; Sahoo, R.R. LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system. *Comput. Netw. Commun. J.* **2019**, *2019*, 205429. [CrossRef]
13. Zhao, J.; Huang, J.; Xiong, N. An effective exponential-based trust and reputation evaluation system in wireless sensor networks. *IEEE Access* **2019**, *7*, 33859–33869. [CrossRef]
14. Michiardi, P.; Molva, R. CORE: A Collaborative REputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. *Adv. Commun. Multimed. Secur.* **2002**, *100*, 107–121. [CrossRef]
15. Buchegger, S.; Boudec, J.L. Performance Analysis of the CONFIDANT Protocol. In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2002, Lausanne, Switzerland, 9–11 June 2002. [CrossRef]
16. Ganeriwal, S.; Srivastava, M. Reputation-based Framework for High Integrity Sensor Networks. *ACM Trans. Sens. Netw.* **2008**, *4*, 1–37. [CrossRef]
17. Pushpalatha, M.; Venkataraman, R.; Ramarao, T. Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks. *World Acad. Sci. Eng. Technol.* **2009**, *56*, 1529–1532.
18. Wang, Y.; Vassileva, J. Bayesian network-based trust model. In Proceedings of the IEEE/WIC International Conference on Web Intelligence, Halifax, NS, Canada, 13–17 October 2003. [CrossRef]
19. Zouridaki, C.; Mark, B.L.; Hejmo, M.; Thomas, R.K. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In Proceedings of the SASN'05, Alexandria, VA, USA, 7 November 2005. [CrossRef]
20. Crosby, G.V.; Pissinou, N.; Gadze, J. A framework for trust-based cluster head election in wireless sensor networks. Proceedings the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, Columbia, MD, USA, 24–28 April 2006. [CrossRef]
21. Xiao, X.; Peng, W.; Hung, C.; Lee, W. Using Sensor Ranks for In-Network Detection of Faulty Readings in Wireless Sensor Networks. In Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access, Beijing, China, 10 June 2007. [CrossRef]

22. Haiguang, C.; Gangfeng, G.; Huafeng, W.; Chuanshan, G. Reputation and Trust Mathematical Approach for Wireless Sensor Networks. *Multimed. Ubiquitous Eng. J.* **2007**, *2*, 521–534. Available online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.190.8855 (accessed on 9 January 2022).
23. Song, F.; Zhao, B. Trust-based LEACH Protocol for Wireless Sensor Networks. In Proceedings of the 2008 Second International Conference on Future Generation Communication and Networking, NW Washington, DC, USA, 13–15 December 2008. [CrossRef]
24. Hui-hui, D.; Ya-jun, G.; Zhong-qiang, Y.; Hao, C. A Wireless Sensor Networks Based on Multi-angle Trust of Node. In Proceedings of the 2009 International Forum on Information Technology and Applications, NW Washington, DC, USA, 15–17 May 2009. [CrossRef]
25. Haiguang, C. Task-based Trust Management for Wireless Sensor Networks. *Int. J. Secur. Its Appl.* **2009**, *3*, 21–26. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.330.7775&rep=rep1&type=pdf (accessed on 9 January 2022).
26. Xiong, L.; Liu, L. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Trans. Knowl. Data Eng.* **2004**, *16*, 843–857. [CrossRef]
27. Mármol, F.G. Providing trust in wireless sensor networks using a bio-inspired technique. *Springer J. Telecommun. Syst.* **2010**, *46*, 163–180. [CrossRef]
28. Awan, S.; Javaid, N.; Ullah, S.; Khan, A.U.; Qamar, A.M.; Choi, J.-G. Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. *Sensors* **2022**, *22*, 411. [CrossRef]
29. Sahoo, S.K.; Mudligiriyappa, N.; Algethami, A.A.; Manoharan, P.; Hamdi, M.; Raahemifar, K. Intelligent Trust-Based Utility and Reusability Model: Enhanced Security Using Unmanned Aerial Vehicles on Sensor Nodes. *Appl. Sci.* **2022**, *12*, 1317. [CrossRef]
30. Alghofaili, Y.; Rassam, M.A. A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. *Sensors* **2022**, *22*, 634. [CrossRef] [PubMed]
31. Tayyab, K.; Karan, S.; Manisha, M.; Mohammad, N.A.; Azlan, M.Z.; Ahmadian, A. Temperature-Aware Trusted Routing Scheme for Sensor Networks: Security Approach. *Comput. Electr. Eng.* **2022**, *98*, 107735. [CrossRef]
32. Zheng, G.; Gong, B.; Zhang, Y. Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6667100. [CrossRef]
33. Sumalatha, M.S.; Nandalal, V. An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN). *J. Ambient Intell Hum. Comput* **2021**, *12*, 4559–4573. [CrossRef]
34. Sivasankarareddy, V.; Sundari, G.; Rami Reddy, C.; Aymen, F.; Bortoni, E.C. Grid-Based Routing Model for Energy Efficient and Secure Data Transmission in WSN for Smart Building Applications. *Appl. Sci.* **2021**, *11*, 10517. [CrossRef]
35. Tayyab, K.; Karan, S.; Mohd, H.; Khaleel, A.; Thippa, R.; Senthilkumar, M.; Ali, A. ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. *Future Gener. Comput. Syst.* **2021**, *125*, 921–943. [CrossRef]
36. The Online Multi-Source Dictionary Search Service, Lexico Publishing Group. Available online: http://dictionary.reference.com/browse/trust (accessed on 9 January 2022).
37. Marmol, F.G.; Perez, G.M. TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009. [CrossRef]
38. ALrahhal, H.; Ramadan, R. A Novel Multi-Threshold Energy (MTE) Technique for Wireless Sensor Networks. *Procedia Comput. Sci.* **2015**, *65*, 25–34. [CrossRef]
39. Jamous, R.; Al-Rahhal, H.; El-Darieby, M. A New ANN-Particle Swarm Optimization with Center of Gravity (ANN-PSOCoG) Prediction Model for the Stock Market under the Effect of COVID-19. *Sci. Program.* **2021**, *2021*, 6656150. [CrossRef]