Fang *et al. J Wireless Com Network* (2021) 2021:14
https://doi.org/10.1186/s13638-020-01884-1

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks

Weidong Fang[1,2], Wuxiong Zhang[1,2,6*], Wei Chen[3], Jin Liu[3,4], Yepeng Ni[5] and Yinxuan Yang[7]

*Correspondence: wuxiong.zhang@main.sim.ac.cn
[1] Science and Technology on Micro-system Laboratory, Shanghai Institute of Micro-system and Information Technology, Chinese Academy of Sciences, Shanghai 201800, China
Full list of author information is available at the end of the article

Abstract

For hierarchical wireless sensor network (WSN), the clustered routing protocol can effectively deal with large-scale application requirements, thereby, how to efficiently elect the secure cluster heads becomes very critical. Unfortunately, many current studies only focus on improving security while neglecting energy efficiency and transmission performance. In this paper, a lightweight trust management scheme (LTMS) is proposed based on binomial distribution for defending against the internal attacks. Simultaneously, distance domain, energy domain, security domain and environment domain are considered and introduced to propose a multidimensional secure clustered routing (MSCR) scheme by using dynamic dimension weight in hierarchical WSNs. The simulation results show that LTMS can effectively prevent a malicious node from being elected as a cluster head, and MSCR can achieve a balance between security, transmission performance and energy efficiency under the requirements of environmental applications.

Keywords: Internet of Things, Wireless sensor network, Security, Routing protocol, Trust management scheme

1 Introduction

The Internet of Things (IoT) is a technology that achieves the connection between things via the Internet. With the rapid development of wireless communication, the wireless sensors are becoming the important components of information collection in IoTs. By using sensors, the devices' operation status or environmental information connected to them can be obtained. Moreover, these wireless sensor nodes are organized into a wireless sensor network (WSN) [1–3]. The sensed information is aggregated and transmitted to the Internet via WSN, and finally, the connections between things are achieved. Currently, WSN can be applied in many fields [4–6], which involve environmental monitoring, smart home, intelligent agriculture and industrial safety monitoring. Therefore, as the important infrastructure, the WSN's network performance directly determines the operation quality of IoT.

In a hierarchical WSN [7–11], a sink node, that is, a cluster head (CH), is usually used to aggregate the sensed information from cluster members, and the clustered routing

protocols are deployed to reduce network traffic and energy consumption. A typical clustered routing protocol, called low energy adaptive clustering hierarchy (LEACH) protocol [12], was proposed to balance the network load and reduce the energy consumption. However, in a hierarchical WSN, if a CH has the higher level, and its data processing load become heavier, the failure of the higher-level CHs may cause the entire network to be paralyzed. Thereby, the balancing load of a hierarchical WSN is a key issue that determines overall network performance. At the same time, if a CH, especially a high-level CH, is captured and compromised, it will impact on the information security of the entire network.

The challenges of information security come mainly from the security attacks [13–16]. In general, these security attacks are categorized into external attacks and internal attacks for WSN. The former involves the probabilistic jamming attacks, the eavesdropping attacks, as well as the decoding attacks. The latter is launched by the compromised node, and its attack behaviors include tampering, discarding, replaying, forging and selective forwarding data packets. The external attacks can be defended against by deploying encryption, authentication, digital watermarking and other traditional security schemes. However, these security technologies cannot defend against internal attacks. This is due to that the compromised nodes have hold the security algorithm and keys. Furthermore, for the resource-constrained sensor nodes, the security algorithms with high computational complexity are almost impossible to execute. Currently, the information security in hierarchical WSNs is mainly improved to ensure the transmission of sensed information in secure by lightweight encryption or authentication schemes. However, due to unattended deployment of sensor nodes, there are no effective schemes to prevent the capture and compromise of nodes. Thereby, the internal attacks that are launched by those compromised nodes are inevitable. Simultaneously, once a malicious node is elected as a CH, the authenticity and integrity of sensed information in the entire cluster will not be guaranteed. Fortunately, some studies have shown that the trust management scheme is an effective approach to defend against the internal attacks [17, 18]. Moreover, we will adopt the trust value from the trust management scheme as a key factor to elect a secure CH, and design a secure routing protocol.

In this context, to meet the requirements of network load balancing and security for the clustered routing protocols, our contributions of this paper include the following:

1. Lightweight trust management scheme (LTMS): by using binomial distribution and adopting CH's recommendations, a novel trust management scheme with low computational complexity is proposed to mitigate the typical internal attack, i.e., collusion attack.
2. Multidimensional secure clustered routing (MSCR): based on the trust value from LTMS, the environment domain, distance domain, energy domain and security domain are introduced to design a secure routing scheme in hierarchical WSNs. It can achieve a balance between energy efficiency, security and transmission performance to prolong the network lifetime.

To compare our contributions with the previous works, the MATLAB is used to simulate and. As a well-known mathematical software, MATLAB is used in data analysis,

wireless communication, deep learning, image processing and computer vision, signal processing, quantitative finance and risk management, robotics, control systems and other fields. The rest of this paper is organized as follows: firstly, the related works on trust management scheme and clustered routing protocols are reviewed and analyzed in Sect. 2. Then, LTMS and MSCR are proposed in Sect. 3. Furthermore, the numerical simulation and analysis are discussed in Sect. 4. Finally, the conclusions are drawn in Sect. 5.

2 Related works

In this section, we will review the recently research on trust management and discuss the secure routing protocols in hierarchical WSNs.

2.1 1.1. Trust management scheme

Existing trust management schemes that employ redemption schemes fail to discriminate between temporary errors and disguised malicious behaviors in which the attacker cleverly behaves well and badly alternatively. Chae et al. presented the vulnerabilities of existing redemption schemes, and described a new trust management and redemption scheme that could discriminate between temporary errors and disguised malicious behaviors with a flexible design. This trust management scheme used a new kind of trust, called predictability trust (PT), which was able to predict future trust values based on past behaviors with an efficient and flexible design. They had shown the analytical results of the trust management scheme and demonstrated the advantages of the proposed scheme with simulation conducted in a WSN. This scheme could provide efficient, secure routing for WSNs [19]. The proposed scheme could defend against on–off attack effectively. However, a dynamic sliding window for bad behaviors in this scheme had no clear definition, and the applicability needed to be improved.

Unattended wireless sensor networks (UWSNs) were characterized by long periods of disconnected operation and fixed or irregular intervals between sink visits. The absence of an online trusted third party implied that existing WSN trust management schemes were not applicable to UWSNs. Ren et al. [20] proposed a trust management scheme for UWSNs to provide efficient and robust trust data storage and trust generation. For trust data storage, they deployed a geographic hash table to identify storage nodes and to significantly decrease storage cost. They used subjective logic-based consensus techniques to mitigate trust fluctuations caused by environmental factors. They also exploited a set of trust similarity functions to detect trust outliers and to sustain trust pollution attacks. Through extensive analyses and simulations, the proposed scheme was efficient, robust and scalable. Although the geographic hash table could significantly decrease storage cost, the hash operation increased computational overhead.

Hussain et al. presented an energy efficient trust management model for securing life-saving information with optimal power/energy consumption by sensor nodes. The proposed model was a cluster-based three-tier architectures, where the first tier recorded the first-run configuration of the nodes. The second tier secured the data between the nodes, and the third tier ensured energy efficiency by calculating energy consumption at every level and rotates cluster head among the nodes. The difficult task of energy efficiency was achieved by the robust algorithm, which configured the nodes and trained

the network by using a machine learning technique. The simulation results showed smooth functioning of the network with less energy consumption. The proposed scheme performed better than anonymous authentication for wireless body area networks with provable security (AAWBAN) in terms of computational overhead, energy consumption, data drop rate and throughput [21]. As one of key research points, the robust algorithm did not provide more explanation on energy consumption, which was generated by configuring the nodes and training the network.

Labraoui et al. presented TMR, a risk-based trust management scheme in WSNs. Compared with the previous schemes, TMR evaluated the overall trust value of a node by the reputation value and the risk value, which was based on interaction-derived information. The risk evaluation was a very helpful component to build the trust model, in order to effectively deal with the conflicting behaviors of the nodes. Through relevant simulation, they got a compelling argument showing the ability of TMR to detect the on–off attack [22]. However, although the maximal value of interactions risk factor between nodes was defined, there were no further explanations on this metric while it acted an important role in direct trust evaluation.

Under the background of equal scale one-hop clustered WSN, according to the behaviors of the sensor nodes within the cluster on event perception, packet forwarding or data fusion, Fang et al. proposed a reputation management scheme based on multi-factor, describing the initialization, update, storage of the reputation value and the punishment and redemption of malicious nodes in detail. The sensor node's reputation value, based on multi-factor, was used to characterize the trustworthiness of sensor node in this scheme. Due to the classification to trust factors constituting nodes' reputation values, and the improvement of calculation methods to reputation values, the objectivity and impartiality were enhanced during the assessment of nodes' reputation values. To verify the effectiveness of the proposed reputation management scheme in identification of distrusted nodes, they applied the reputation management scheme to the existing SPIN routing protocol to obtain a new trust enhanced routing protocol, called SFA [23]. The punishment and redemption for malicious nodes were the common trust decision schemes. It directly determined how the compromise node was processed. In SFA, how to punish and redeem those malicious nodes lacked further descriptions.

The information security is always a trending topic in WSNs. Even if the classic trust management based on BETA distribution and its improved model proposed recently might detect the internal attacks, it still lacks an effective defense mechanism to prevent the on–off attack of malicious nodes. Hence, according to the Gaussian distribution, Zhou et al. introduced the trust management system and the novel method included the controlling factor to defend against the on–off attacks in WSNs. In Gaussian trust management scheme (GTS), the cost of on–off attacks was mitigated by using the controlling factor, and the malicious nodes were detected. Through some preliminary simulation results, this model was more stable to describe reputation against other distributions and easier to display the trust directly and sensitively, and it also had the powerful ability to prevent from on–off attacks [24]. The parameter—penalty, had no clear quantification based on different scenarios.

Kowshalya and Valarmathi proposed a trust management scheme to facilitate trustworthy automatic decision making based on behaviors of objects. They used social

Internet of Things (SIoT) trust metrics, namely direct trust, centrality, community interest, cooperativeness, service score, expected trust, overall trust and trust updates, to compute trustworthiness among objects. The expected trust and periodic trust were updated evidently to detect the selective forwarding attacks. They demonstrated the advantages of the proposed scheme with other existing trust management schemes and pointed out the other trust management schemes under study took a longer duration to detect on–off attacks due to lack of expected trust [25]. There were larger computational cost and communication overhead in proposed scheme.

Wu et al. proposed a beta and link quality indicator (LQI)-based trust model (BLTM) for WSNs. When a direct trust is calculated, they considered communication trust, energy trust and data trust. Then, the weights of these factors were discussed. At last, they also proposed an LQI analysis mechanism is to maintain the accuracy and stability of the trust value for normal nodes with poor-quality links. Compared with the beta-based trust and reputation evaluation system (BTRES) [18], the simulation results had shown that BLTM can defend against denial of service (DoS) attack and data tampering attack, and the trust value of normal nodes can maintain stable and accurate [26]. Obviously, the link quality indicator was an important parameter in PHY. Not every low-cost microcontroller unit (MCU) of sensor node could obtain this indicator.

Han et al. proposed a synergetic trust model based on support vector machine (SVM), called STMS, to achieve accurate and robust trust evaluation for an underwater acoustic sensor networks (UASNs). The STMS is made up of three parts. (1) Three kinds of trust evidences are generated and refined by cluster members. (2) By using SVM technology, a trust prediction model was trained to evaluate accurate trust value. (3) The scheme of double cluster heads was designed to enhance network security and prolong the network lifetime. Simulation results demonstrated that, in the aspect of detect accuracy of malicious nodes, success rate of communication and network lifetime, STMS performed better than other related works in the sparse deployment environment [27]. Considering the constrained resources of underwater acoustic sensor, the complexity of proposed model needed to be evaluated.

In healthcare-oriented wireless sensor network (HWSN), it is also facing enormous security challenges, especially from internal attacks. It is difficult to distinguish many attack behaviors from interference in the complex healthcare scenarios, such as on–off attack. Fang et al. proposed a binomial distribution-based trust management scheme (BDTMS) for HWSN. The proposed method could rapidly detect and effectively defend against on–off attacks and bad mouthing attacks. The trust value of the node was evaluated. Simulation results showed that, compared with the time-window-based resilient trust management scheme (TRTMS) [17], the proposed BDTMS achieved better performance in defending against on–off attack under obstacle movement, especially with higher detection accuracy [28]. In BDTMS, the speed of obstacles did not be considered.

As mentioned above, the deferent trust management schemes/models are designed to meet different security requirements in WSNs. However, the energy consumption often seems to be ignored, while this is very important for resources-constrained nodes. Currently, most existing trust management schemes are based on trust/reputation evaluation. The application of trust management in wireless sensor networks is mainly aimed at the following aspects: (1) against attacks in the network, (2) identifying malicious

nodes and detecting malicious behavior, (3) improving the security of data storage. The scholars evaluate the proposed scheme through metrics such as accuracy, robustness, energy consumption, throughput, calculation overhead and data loss rate. In conclusion, the introduction of trust management provides higher security and higher efficiency for wireless sensor networks.

2.2 1.1. Secure LEACH

Although LEACH protocol can improve energy efficiency, there was no any security algorithm in this routing protocol. Subsequently, some improved LEACH protocols with security were proposed.

The goal of the proposed secure data transmission for hierarchical WSNs was to guarantee a secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the base station (BS). In the proposed approach, the election of new cluster heads was from the nodes with the highest remaining energy. Then, the current cluster head informed the base station about the authenticity of the elected cluster head. The message from the cluster head to the based station was encrypted by MAC algorithm with the shared key between the base station and the cluster head. After that, the BS broadcast the list of the authenticated cluster heads to all nodes using uTESLA. After broadcasting the list of the authenticated cluster heads, nodes could initiate a joint request to one of the cluster heads. By using NS-2.35, the simulation results showed that, after improving LEACH protocol power consumption and adding the security measures, the approach performed better in terms of the system throughput, network lifetime, data transmitted and the total energy consumption. The proposed approach provided a secure authentication solution for the network [29]. However, the shared key was managed and updated would consume too much energy.

All the different key management schemes in WSNs, the deterministic key management scheme with LEACH called DKS-LEACH was the scheme, which was used to secure wireless sensor network in efficient manner and provided authentication, confidentiality and integrity of sensed data. There were still some issues with DKS-LEACH like energy consumption and resilience against node capture. Barad and Kadhiwala proposed a DIST-LEACH scheme to improve the existing scheme to make it more resilient using distance-based key management scheme. They had provided a performance analysis of the proposed scheme, including energy consumption and resilience against compromised node. The results showed that even in case of compromised node attack the proposed scheme provided better residual energy and better resilience [30]. The communication overhead on the key management needed to further analyze in DKS-LEACH.

The LEACH protocol lacked of security support. Patel and Jinwala proposed an improvement of LEACH, called E-LEACH (end-to-end secure LEACH) which uses homomorphic encryption to provide secure data aggregation in wireless sensor networks. Due to the algebraic characteristics in homomorphic encryption, the transmitted data could be algebraically aggregated without decryption and hence require least amount of energy, while ensuring privacy. E-LEACH provided data authentication, data confidentiality and data integrity along with privacy, and also provided robustness against node capture attack as keys were generated by seed value broadcasted by BS and not remained persistent in memory. Hence, after reset of a node, an attacker would

not gain any seed-related information. E-LEACH was compared to LEACH in terms of energy consumed [31]. However, the additional energy consumption due to encryption did not be analyzed.

The nodes in WSNs had limited computational ability and limited energy. These device constraints dictated the choice of various crypto primitives for the security model. Kodali et al. considered a stream cipher algorithm, RC-4, which was easy to implement on the sensor devices fast enough. Hence, it was chosen for the performance evaluation of multi-level secure LEACH. In general, the RC-4 used a static key for the encryption and decryption processes. This static key was replaced by a dynamic key, which was computed using the Toeplitz hash function in making the security model further sturdier. The security overhead due to RC-4 on the life-time of the network had been analyzed by developing a model for LEACH protocol. The average energy of the network and the number of dead nodes were evaluated under three different levels models for LEACH protocol. These results showed that levels 1, 2 and 3 without security fare better than level 1, 2 and 3 models when security was included. Also, higher level LEACH performed better than the lower levels of LEACH [32]. Toeplitz Hash algorithm was more suitable for multi-process load balancing, and it could not apply in single-process MCU.

Mezrag et al. proposed a new secure protocol based on the LEACH routing protocol named hybrid cryptography-based scheme for secure data communication in cluster-based WSN (HCBS). As a multi-constrained criteria approach, HCBS was built on a combination of the cryptography technique based on elliptic curves to exchange keys that used symmetric keys for data encryption and MAC operations. After a set of tests on TOSSIM simulator, the results obtained showed that the proposal achieved good performances in terms of energy consumption, average packet loss rate and end-to-end delay compared with SecLEACH. In addition, HCBS guaranteed a high level of security [33]. Although the cryptography technique based on elliptic curves had high security strength, it is difficult to support the long-term operation of WSN.

Saadawy and Shaaban proposed MS-LEACH to enhance the security of SLEACH by providing data confidentiality and node to cluster head (CH) authentication using pair-wise keys shared between CHs and their cluster members. The security analysis of proposed MS-LEACH showed that it had efficient security properties and achieves all WSN security goals compared to the existing secured solutions of LEACH protocol. A simulation-based performance evaluation of MS-LEACH demonstrated the effectiveness of proposed MS-LEACH protocol and showed that the protocol achieves the desired security goals and outperforms other protocols in terms of the energy consumption, the network lifetime, the network throughput and the normalized routing load [34]. The pair-wise keys shared between CHs and their cluster members could defend against the external attacks instead of the internal.

In order to save node energy and enhance wireless sensor network security, the LEACH protocol has been improved. Zhang and Wei presented a routing protocol based on clusters in which the sensing area consists of a number of equilateral hexagons called clusters, and each of clusters had six equilateral triangles called cells. All cells had equal number nodes and then all clusters had equal number nodes. The cell heads were selected in each cell and then a cluster head was chosen from those six cell heads. The data were sent to the base station through employing a multi-jumping

manner along a routing path consisting of cluster heads. In a certain grid, nodes established pair-wise keys by utilizing the polynomial key management and ID-based key management. The arithmetic balanced energy expense among all the nodes, saved the node energy and prolonged the life of wireless sensor networks. Additionally, this arithmetic improved the security of the wireless sensor network [35].

Wang et al. put forward a kind of secure LEACH routing protocol (SC-LEACH) based on low-power CH selection algorithm. This protocol got the total number of all nodes by their collaboration in selecting, to precisely calculate the present thresholds with which the cluster heads are generated. Consequently, the probability of producing optimal cluster heads in each round was the biggest, and the variance was the smallest; thus, the network reached its optimal energy cost. The adoption of pre-shared key pair dispatch improved the security of the routing effectively. The performance of the two algorithm were compared synthetically by the following five index: survived nodes in every round, total energy cost of all nodes, cluster heads produced in every round, average energy cost of every round, sample second-order central moments of the CHs in every round. Comparing with the LEACH protocol using the symmetric keys dispatch, they validated the effectiveness of SC-LEACH by simulation. SC-LEACH protocol used pre-shared key pair, so it was certainly much more secure than LEACH protocol using the symmetric keys dispatch [36].

To address the issues of the early death of nodes, Zhou et al. proposed an improved LEACH target location constraint (LEACH-TLC) algorithm. In this algorithm, a network monitoring performance parameter model was constructed to obtain the wake-up/dormant threshold of the network node. Moreover, by using this threshold, the dormant strategy of node was designed to establish the working node set. Finally, combined with the distance factor between this node and BS, a new cluster head selection rule was proposed. The LEACH-TLC algorithm could reduce the number of working nodes and energy consumption of the network, balance the energy consumption distribution of the nodes and prolong network lifetime [37].

As a cluster-based routing protocol, LEACH is widely used in WSNs. Amirthalingam and Anuratha proposed an improved LEACH protocol, named I-LEACH. This proposed protocol improved the algorithm of electing cluster head nodes for LEACH protocol. They considered the LEACH protocol relied on random threshold probability to elect cluster head nodes, and then designed and introduced two score functions for energy consumption and the distance from BS. The two score functions were weighted and then summed, and then, the random threshold probability is added. Multiply to get the new threshold probability function [38]. However, because it does not consider security issues, WSNs are vulnerable to attacks, affecting the security of the network. Therefore, many researchers have improved LEACH. Most researchers use encryption and authentication algorithms to protect data, thereby increasing network security. Protocols are usually evaluated using metrics such as energy consumption, network lifetime and packet delivery rate. However, the secure routing protocols improve network security at the expense of energy efficiency. Simultaneously, many secure LEACHs are based on the assumption, which is the CH is trusted, while this assumption cannot be guaranteed in practical applications of WSN.

3 Multidimensional secure clustered routing scheme

3.1 Lightweight trust management scheme

Generally, the binomial distribution is n repeated Bernoulli trials. The success or failure of each Bernoulli trial is taken as the success (cooperation) or failure (non-cooperation) number of the interaction between the nodes in WSNs. The node's reputation can be defined as the probability distribution function of binomial distribution. The reputation value is updated by continuous interaction between nodes to calculate the new trust value. Binomial distribution is a probability distribution mainly describing the distribution of discrete events, which is usually composed of two mutually exclusive events. Beta distribution refers to a set of continuous probability distributions defined in the interval (0, 1). The Poisson distribution mainly describes the number of random events that occur per unit time. The relationships between above three distribution are that the binomial distribution can be regarded as the counterpart of Poisson distribution in discrete time, and Beta distribution can be approximated as the binomial distribution when $n=1$. Due to the low computational complexity and storage space, this is, only cooperation or non-cooperation numbers are recorded and calculated in Bernoulli trial, and it is suitable for the resource-constrained sensor nodes to represent their interaction behaviors [39].

1. Binomial distribution and reputation value

Considering a binomial distribution $\mathrm{Bin}(n,k)$ represents the probability of k successes in n repeated Bernoulli trials. $\mathrm{Bin}(n,k)$ can be expressed as follows:

$$\mathrm{Bin}(n,k) = \frac{n!}{k!(n-k)!}p^k(1-p)^{n-k} \tag{1}$$

where p is the probability of successes. Because there is cooperation or non-cooperation in an interaction between nodes, the binomial distribution can be introduced to describe the interaction behaviors. Here, we assume that the node i and node j interacted $a+b$ times, a represents the cooperation number, b is the non-cooperation number, and assume the probability of cooperation is p. Therefore, the reputation value $R_{i,j}$ of node i to node j is expressed by using the binomial distribution.

$$R_{i,j} = \mathrm{Bin}(a+b,a) = \frac{(a+b)!}{a!b!}p^a(1-p)^b \tag{2}$$

2. Direct trust value

Since $R_{i,j}$ is the probability distribution function, and its maximum value represents the greatest probability of p, thereby, the maximum value is defined as the trust value of node i to node j, this is, the direct trust value $DT_{i,j}$.

$$R'_{i,j} = \left[\frac{(a+b)!}{a!b!}p^a(1-p)^b\right]' = 0 \tag{3}$$

$$p = \frac{a}{a+b} \tag{4}$$

where $p=1$ and $p=0$ represent maximum and minimum values, respectively. Hence, $DT_{i,j}$ is expressed as:

$$DT_{i,j} = \frac{a}{a+b} \tag{5}$$

3. Trust initialization

Generally, the trust values of all nodes in WSNs are defined as the same initial value, and all nodes are normal. We assume that the trust value is 0.5 for each node, and a is equal to b. Both of them are not 0.

In the initialization phase, if a and b are set to smaller, this is, there are few interactions between node i and node j. The obtained trust values are evidently not accurate enough. For example, when interference occurs, the interaction failure is caused by non-malicious nodes, and the evaluation of the trust value has a greater impact. In contrast, if a and b have larger values, the historical weight will be increased. It will impact on the subsequent trust evaluation eventually. The convergence time for the trust value will become longer, and it may affect the normal operation of the network. Thereby, the initial a and b should be set the appropriate values. Usually a and b are set to 5.

4. Trust synthesis

To achieve the objectivity of trust value, we introduced CH's recommendations as the indirect trust value. We assume that the current cluster head is secure, and its behaviors are trusted. We represent the direct trust value of CH to node j as $DT_{CH,j}$. Hence,

$$IT_{i,j} = DT_{CH,j} \tag{6}$$

Meanwhile, an indirect trust weight w_{ind} $0 \le w_{ind} < 1$ is introduced to synthesize the final trust value $T_{i,j}$.

$$T_{i,j} = (1 - w_{\text{ind}}) \times \text{DT}_{i,j} + w_{ind} \times \text{IT}_{i,j} \tag{7}$$

$$w_{ind} = \begin{cases} 0.5 & \text{if } \left|\text{DT}_{i,j} - \text{IT}_{i,j}\right| < \xi \\ \frac{\left|\text{DT}_{i,j} - \text{IT}_{i,j}\right|}{\text{DT}_{i,j}} & \text{else if } \xi \le \left|\text{DT}_{i,j} - \text{IT}_{i,j}\right| < 1 \text{ and } 0.5 < \text{DT}_{i,j} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

where ξ represents a deviation between the direct trust value and the indirect trust value. Usually, ξ is less than 10% of the initial trust value. The synthesized indirect trust value can defend against the slander attacks. Due to the CH's trustworthiness, the collusion attacks can be mitigated effectively.

3.2 Environment domain

Generally speaking, in many improved schemes for cluster head election, the residual energy of node and the distance between node and BS are considered and introduced to elect an optimal cluster head. Nonetheless, we have noticed that the environment domain is an important factor for large-scale WSN. This is due to the fact that the local harsh environment will impact on the transmission of information. If a node with poor external environment is elected as a cluster head, it will affect the stable operation of the network and shorten the network lifetime. Hence, we study the environmental factor, which expresses as follows:

$$E_{\text{env}}^{k}(i) = \begin{cases} 0 & M^{k}(i) < M_{\min}^{k} \\ N^{M(i)-M_{\min}^{k}} - 1 & M_{\min}^{k} \le M^{k}(i) < M_{L}, N > 1, M_{L}^{k} = \log_{N} 2 + M_{\min}^{k} \\ 1 & M_{L}^{k} \le M^{k}(i) \le M_{H}^{k} \\ N^{M_{\max}^{k}-M(i)} - 1 & M_{H}^{k} < M^{k}(i) \le M_{\max}^{k}, N > 1, M_{H}^{k} = M_{\max}^{k} - \log_{N} 2 \\ 0 & M_{\max}^{k} < M^{k}(i) \end{cases} \tag{9}$$

where $E_{\text{env}}^{k}(i)$ is an environmental domain parameter created by the sensor node i for environmental factor k, which represents temperature, humidity or radiation. $\left[M_{L}^{k}, M_{H}^{k}\right]$ is the normal operating interval of the sensor node i for the environmental factor k. If the environmental data collected by the node ($M^{k}(i)$) is within the range $\left[M_{L}^{k}, M_{H}^{k}\right]$, it can be considered that the performance of the sensor node i will not be affected by environmental factors k. So, $E_{\text{env}}^{k}(i)$ is set to 1. Otherwise, it will be reduced, and the negative influence of environmental factors k on nodes i tends to be more obvious. In order to standardize a single environmental field, we have introduced and as the boundary of environmental factors $M_{\min}^{k}$ and $M_{\max}^{k}$, which means that the sampled data of the factor is only allowed in $\left[M_{\min}^{k}, M_{\max}^{k}\right]$. A single environmental domain function is expressed in Eq. (9).

3.3 Security domain

To enhance the security, we introduce the trust values as one of the dimensions in the electing cluster head phase. The candidate cluster head nodes in the current round process take into account the trust value factor of the last round of cluster head distribution to the nodes in the cluster. The trust value is obtained by Eq. (8). We define TV_{ave} is all nodes' average trust value in the last round of cluster. The security domain for node j is represented by $S_{\text{TV}}(j)$, which is expressed as the following expression:

$$S_{\text{TV}}(j) = \frac{T_{i,j} - \text{TV}_{\text{ave}}}{\text{TV}_{\text{ave}}} \tag{10}$$

when an abnormality is detected for a node, which trust value may be much lower than TV_{ave}, and then $S_{\text{TV}}(j) < 0$, so that reduces the probability of a malicious node being elected as the cluster head.

3.4 Multidimensional secure clustered routing

In classic LEACH, the probability that a normal node becomes a cluster head is set by experience in advance, and there is great uncertainty. There is no way to ensure that malicious nodes are not elected as cluster heads simultaneously. In this subsection, we will introduce the security domain and the environment domain into the multidimensional secure clustered routing (MSCR) scheme. The energy domain and the distance domain are considered into MSCR. A novel threshold function for the cluster head election in the current round is calculated as follows:

$$T(\mathrm{i}) = \begin{cases} \frac{P}{1-P(r \bmod \frac{1}{P})}\left(\omega_{\mathrm{eng}} \times \frac{E_{\mathrm{res}}(j)}{E_{\mathrm{eng}}(j)} + \omega_d \times \frac{d_{\mathrm{BS}}(j)}{d_{\mathrm{BS-max}}} + \omega_{\mathrm{env}} \times E_{\mathrm{env}}^k(i) + \omega_{\mathrm{TV}} \times S_{\mathrm{tv}}(j)\right), & \text{if } i \in G \\ 0, & \text{if } i \notin G \end{cases} \tag{11}$$

where $E_{res}(j)$ is the current energy value of the node j. $E_{\mathrm{eng}}(j)$ is the initial energy value of the node j. $d_{\mathrm{BS-max}}$ is the maximum distance from nodes to BS. $d_{\mathrm{BS}}(j)$ is a distance from node j to BS. P represents the probability that the sensor node defaults to the cluster head node, G represents a group of sensors that have not become a cluster head node during the previous $(1/P)$ round, and r represents the current round process. ω_{eng}, ω_d, ω_{env} and ω_{TV} are the dimension weights, which represent the energy domain, the distance domain, the environment domain and the security domain, respectively. They satisfy the following expression:

$$\omega_{\mathrm{eng}} + \omega_d + \omega_{\mathrm{env}} + \omega_{\mathrm{TV}} = 1 \tag{12}$$

The operation process of MSCR is shown as follows:

Step 1 In the first round, the cluster head selection phase and the stabilization phase of the LEACH are directly performed. The current information (including trust value) of each cluster member is transmitted to the BS through the control packet through via cluster heads. The E_{eng} and d_{BS} of each node can be obtained. Usually, ω_{eng}, ω_d, ω_{env} and ω_{TV} are set as 0.25, respectively.
Step 2 Based on the received information, the BS calculates and broadcasts $\mathrm{TV}_{\mathrm{ave}}$.
Step 3 Each cluster member broadcasts a control packet to a node within a preset radius of the cluster and simultaneously confirms the number of neighbor nodes by the number of received control packets;
Step 4 Each cluster member qualifies to be a cluster head node compared with Eq. (11) threshold function to determine whether it can become the cluster head of the current round process.
Step 5 The stabilization process is based on the LEACH protocol. The nodes in the cluster transmit the collected information and the current node information (including trust value) to the cluster head through the data packet and control packet, respectively, and the data are compressed by the cluster head and transmitted to the BS.
Step 6 Repeating the steps from Step 2 to Step 5.
Step 7 This algorithm ends when there are too many nodes dying.

4 Mathematical experiment and discussion

In this section, the proposed MSCR will be simulated and analyzed to compare with LEACH, I-LEACH and LEACH-TLC. The energy consumption, the network lifetime and the data packets transmission are taken as the evaluation metrics.

4.1 Experimental methods

In this subsection, the MATLAB is used to simulate and compare our proposed protocol with LEACH, I-LEACH and LEACH-TLC. To conveniently understand the results, we provide explanations of the following terms. The network lifetime is represented as the number of alive nodes, and the first node dead (FND) and ENL (End of Network Lifetime) were further measured by four algorithms. The ENL refers to the dead nodes exceeding 98% of the total nodes. In addition, in order to verify the impact of the introduced trust values on security, the security attack, i.e., discarding data packets, will be regarded as interferences to impose on the network during certain periods of time during protocol operation. The specific simulation parameters are shown in Table 1.

The impact of environment domain (wildfire, heavy rain) uses a radiation model [40]. In this model, the impact of the environmental event decreases with increase in distance from the center of the event. In environment domain, the temperature of the event center will inevitably destroy the sensor node, and as the distance increases, the temperature will become lower, and the failure probability of the sensor node will also decrease accordingly. Rainstorm events adopt the uniform distribution pattern of natural observation. In this model, the event area is massive, and the impact of the event on the sensor nodes in the area is exactly the same. Depending on the severity of the rainstorm, the affected nodes will experience performance degradation or complete failure.

For the convenience of analysis, the threshold functions of LEACH [12], LEACH-TLC [37] and I-LEACH [38] are shown in Eqs. (13), (14) and (16), respectively. In LEACH, the principle for electing cluster heads is to randomly generate a random number between 0 and 1. If the generated random number of a node is less than the threshold value $T(i)$, the node is elected and announced as the cluster head. In each round, if a node has been elected as the cluster head, then set $T(i)$ to 0, so that the node will not be repeatedly

Table 1 Simulation parameters

Parameters	Value
Nodes number	100
Sensed area	$200 \times 200\ m^2$
BS coordinate	(100, 100)
Initial energy	0.1 J
Length of data packet	4000 bit
Initial environment domain value	1
P	6%
Number of rounds	1000
sE_{elec}	$50\ nJ/bit/m^{-1}$
E_{DA}	$5\ nJ/bit/m^{-1}$
ε_{fs}	$0.0013\ pJ/bit/m^{-4}$
ε_{mp}	$10\ pJ/bit/m^{-2}$

elected as the cluster head. For the node that has not been elected as the cluster head, it will be elected with the probability of $T(i)$. When the number of cluster head nodes increases, the probability of the remaining nodes being elected increases as the cluster head, this is, the threshold $T(i)$ increases, and the probability of a node generating a random number less than $T(n)$ also increases. When there is only one node that is not elected as the cluster head, $T(i)$ is set to 1. Here, $T(i)$ can be expressed as:

$$T(i) = \begin{cases} \frac{P}{1-P\left(r \bmod \frac{1}{P}\right)}, & \text{if } i \in G \\ 0, & \text{if } i \notin G \end{cases} \tag{13}$$

where P is the proportion of cluster heads in all nodes, r is the current round, and $r \bmod \frac{1}{P}$ represents the number of nodes that have been elected as cluster heads in this round. G is the set of nodes that have not been elected cluster heads in this round.

$$T(s_i) = \begin{cases} P + \Delta T(s_i) + (1/n) \sum_{i=1}^{n} (\Delta T(s_i)), & \text{if } i \in G \\ 0, & \text{if } i \notin G \end{cases} \tag{14}$$

Here,

$$\Delta T(s_i) = \alpha E_{\text{pavg}}(s_i) + \beta(1 - \omega_{\text{st}}(s_i)) + \gamma(1 - \omega_{\text{ss}}(s_i)) \tag{15}$$

where P is the desired percentage of CHs in a WSN, $\Delta T(s_i)$ is the threshold compensation value that the node s_i becomes the CH, $E_{\text{pavg}}(s_i)$ is the RE rate of the node s_i, ssss$\omega_{\text{st}}(s_i)$ is the distance factor between the target and node s_i, $\omega_{\text{ss}}(s_i)$ is the distance factor between the node s_i and the BS, and α, β, γ represent the weight factors of the threshold, their values are changing with the monitoring area, the monitoring environment and the energy consumption of the nodes,

$$T(i) = w_1 \left[\frac{E_{\text{current}}}{E_{\max}}\right] + w_2 \left[\frac{d_{\text{BS}}}{d_{\text{far}}}\right] \begin{cases} \frac{P}{1-P\left(r \bmod \frac{1}{P}\right)}, & \text{if } i \in G \\ 0, & \text{if } i \notin G \end{cases} \tag{16}$$

where $w_1 + w_2 = 1$, and both of them are given according to the preference for the energy and distance of the network. d_{BS} is distance between the node and BS, and d_{far} is distance to the BS from the farthest node of the cluster. E_{current} represents the residual energy of a node, and $E_{\max}$ represents the maximum energy of a node. For LEACH-TLC and I-LEACH, their $T(i)$s decrease based on the requirements of load balancing to further improve the energy efficiency. Thereby, how to reasonably reduce $T(i)$ to meet the energy efficiency and security requirements is also our concern.

4.2 Results and discussion

The experimental results are shown in Figs. 1, 2 and 3. The results will be discussed in energy consumption, network lifetime and data packets transmission, respectively.

1. Energy consumption

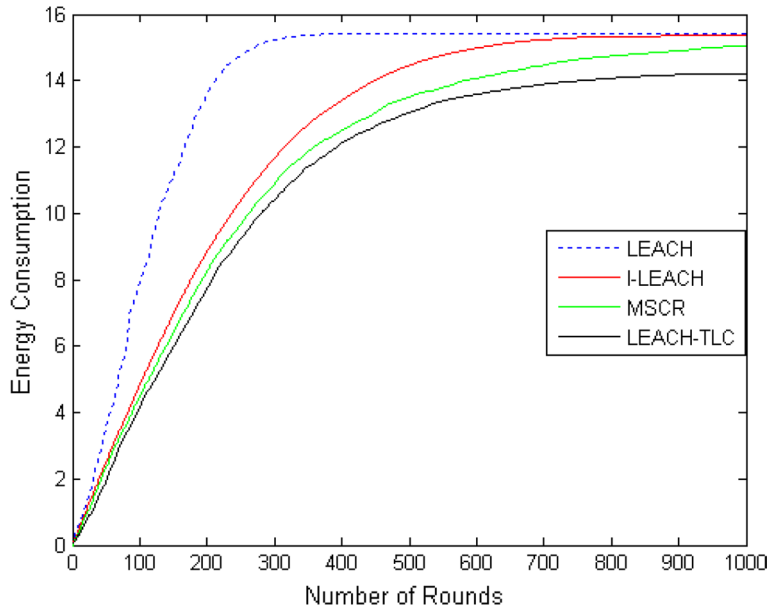

Fig. 1 Comparison of energy consumption

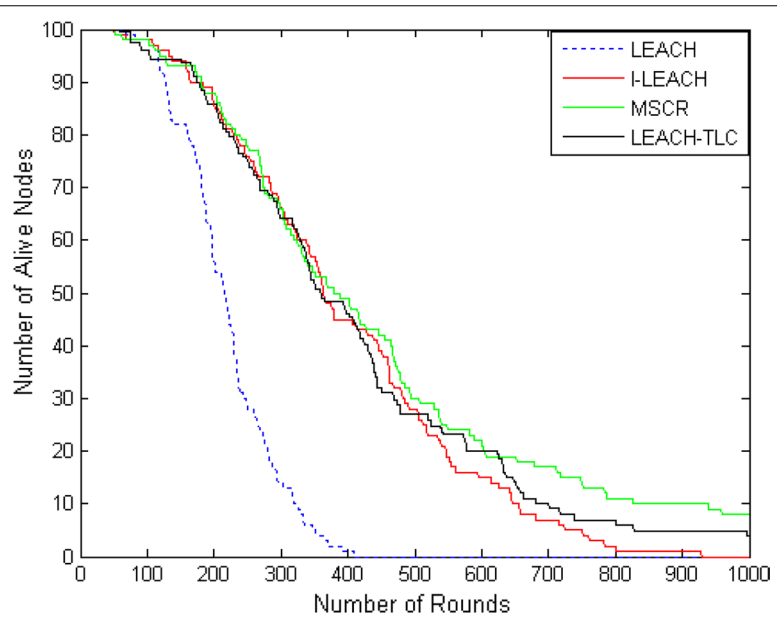

Fig. 2 Comparison of network lifetime

The energy consumption of sensor nodes in LEACH, I-LEACH, LEACH-TLC and MSCR will change with the network operation time. As the network working time increases, the sensor node energy consumption gradually increases. When the network starts operating, the difference between the energy consumption of the four protocols is small within a short period of time. Subsequently, the energy consumption increases sharply with the increase of the operating time, and the difference gradually increases. It

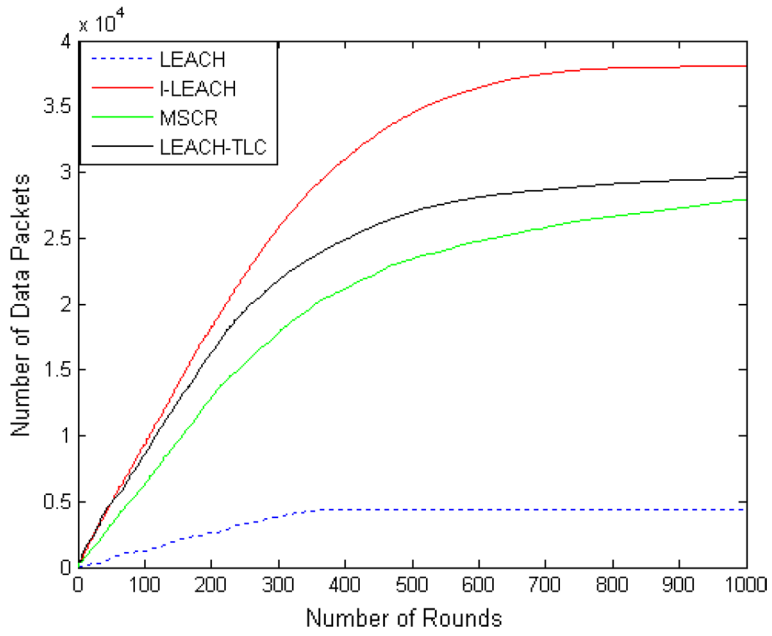

Fig. 3 Comparison of data packets transmission

can be clearly seen that the energy consumption of LEACH is always higher than MSCR, LEACH-TLC and I-LEACH. Due to the dormant strategy of node, the energy consumption of LEACH-TLC is the smallest in the four protocols.

When the network operation reaches the middle stage, all of them consume a large amount of energy. The energy consumption is relatively slow in the middle stage to end stage. It can be seen in Fig. 1 that MSCR, LEACH-TLC and I-LEACH have lower energy consumption. This is due to that the energy consumption and transmission are both taken into account. Among them, the MSCR also has environmental awareness, which can make it avoid dangerous areas and elect more suitable node as CH. Therefore, MSCR has the lowest energy consumption. In LEACH, when the network operates to about 280 rounds, its residual energy is only 7%. When the network operates to 596 rounds in I-LEACH, the residual energy is 7%. When the network operates to 1000 rounds in MSCR and LEACH-TLC, the residual energy is still 10% and 12%, respectively.

2. Network lifetime

The curves of the number of alive nodes with the network operation time are shown in Fig. 2 based on LEACH, I-LEACH, LEACH-TLC and MSCR. In Fig. 2, the FND of LEACH appeared in the 56th round until the ENL in the 420th round, and the FND in I-LEACH appeared in the 70th round until there were about 5 nodes left in the 800th round. For MSCR, the FND appeared in the 82nd round. Until the 1000th round, about 8 nodes are still alive. For LEACH-TLC, the FND appeared in the 95nd round. Until the 1000th round, about 5 nodes are still alive.

In Table 2, it has shown the comparison with the FND and ENL of LEACH, I-LEACH, LEACH-TLC and MSCR. The data were averaged for multiple simulations. The FND

Table 2 Comparison of network lifetime

Protocol	Round of FND	Round of ENL
LEACH	56	420
I-LEACH	70	930
LEACH-TLC	95	1000+
MSCR	90	1000+
Improved	61%	114%

in I-LEACH appeared later, and its network stability increased by 25% compared to LEACH. Meanwhile, compared with LEACH, the network stability of MSCR and LEACH-TLC had increased by 61% and 69%, respectively, and both of network lifetimes had extended by 138%. When the simulation ended, the number of alive nodes in MSCR is more than the number of alive nodes in LEACH-TLC. This is due to the fact that the consideration of security could enhance the availability during a long term operation of the network.

This is due to that, I-LEACH, LEACH-TLC and MSCR consider energy consumption and distance to make energy consumption more balanced, the network lifetimes of the three are longer than LEACH. However, I-LEACH and LEACH-TLC do not consider the impact of environmental factors, and the cluster head node cannot be avoided to avoid dangerous areas, so the network lifetime is shortened. In contrast, MSCR can better extend the network lifetime because of its environmental awareness.

3. Data packets transmission

In Fig. 3, the comparison of data packets transmission of four protocols demonstrates that the transmitted data packets in MSCR are much higher than the LEACH. The transmitted data packets in I-LEACH and LEACH-TLC are about 15% and 11% higher than MSCR, respectively. This is because the latter has the overhead of the security domain and environment domain. For WSN, the secure and reliable transmission of data should be considered essentially with lower energy consumption and longer network lifetime. Hence, the reduction of data packets can be tolerated to a certain extent.

5 Conclusions

For large-scale wireless sensor network, a single planar routing protocol in the network has not only a slow convergence rate, but also a complex network topology reduces the reliability and accuracy of the data transmission process, although it has better robustness. Therefore, both simplifying the network topology and improving the transmission efficiency in secure need to be considered comprehensively. In general, the network is self-governed by a hierarchical routing protocol, which can effectively cope with large-scale application scenarios. The improvement of security in hierarchical routing protocols mainly depends on the deployment of traditional security scheme such as encryption or authentication. However, the constrained resources of sensor node limit the application of high-strength security algorithms, the encryption and authentication schemes cannot defend against the internal attacks. Thereby,

we try adopting the trust value into the design of hierarchical routing protocol, and look forward to improving transmission security and preventing the internal attacks while reducing computing overhead.

The contribution of this paper is to propose a multidimensional secure clustered routing scheme,(MSCR), which can improve the availability of the network, prolong the lifetime of the network and enhance the network security. By using the residual energy, distance and environment factors, the size of the cluster can be better constrained to improve energy efficiency, and avoid excessive energy consumption of a node. Simultaneously, the LTMS is introduced into MSCR. Specifically, the related attributes of the trust value are introduced in the cluster head election process, so that the protocol is improved in energy efficiency and the security is also enhanced accordingly.

The simulation results showed that MSCR outperforms LEACH-TLC, I-LEACH and LEACH in prolonging the network lifetime and balancing energy consumption. It can be seen from the simulation experiment of the number of data packets that the introduction of trust value in binomial-based trust management scheme can effectively mitigate the influence of malicious nodes on cluster head election, which can greatly guarantee the security of the overall network. In the near future, we will research and analyze the impact of different distributions on secure routing protocols in hierarchical wireless sensor networks.

Abbreviations

IoT: Internet of Things; WSN: Wireless sensor network; CH: Cluster head; BS: Base station; LTMS: Lightweight trust management scheme; MSCR: Multidimensional secure clustered routing; LEACH: Low energy adaptive clustering hierarchy; I-LEACH: Improved LEACH; AAWBAN: Anonymous authentication for wireless body area networks; PT: Predictability trust.

Acknowledgements

We are grateful to the anonymous reviewers who have contributed to the enhancement of the paper's completeness with their valuable suggestions.

Authors' contributions

The six authors of the paper have extensively participated in all of the paper writing. WF mainly worked on the researched. WZ, WC and JL revised this paper. YN and YY mainly added to and revised the related works. All of the authors equally contributed to reviewing the manuscript.

Funding

This research was funded by the National Natural Science Foundation of China (Grant Nos. 51874300, 61571303), the National Science and Technology Major Project of China (Grant No. 2018ZX03001031), the National Natural Science Foundation of China and Shanxi Provincial People's Government Jointly Funded Project of China for Coal Base and Low Carbon (Grant No. U1510115), the Qing Lan Project, the China Postdoctoral Science Foundation (Grant No. 2013T60574), the Shanghai Municipal Key Project (Grant No. 19511132401), the Shanghai Municipal Natural Science Foundation (Grant No. 18ZR1437600), the Fundamental Research Funds for State Key Laboratory of Synthetical Automation for Process Industries (Grant No. PAL-N201703) and the National Key Research and Development Program of China—Internet of Things and Smart City Key Program (Nos. 2019YFB2101600, 2019YFB2101602, 2019YFB2101602-03).

Availability of data and materials

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

[1] Science and Technology on Micro-system Laboratory, Shanghai Institute of Micro-system and Information Technology, Chinese Academy of Sciences, Shanghai 201800, China. [2] University of Chinese Academy of Sciences, Beijing 100049, China. [3] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China. [4] School of Engineering and Information Technology, University of New South Wales, Canberra 2610, Australia. [5] School of Data Science and Media Intelligence, Communication University of China, Beijing 100024, China. [6] Shanghai

Research Center for Wireless Communication, Shanghai 201210, China. [7] Fuzhou Internet of Things Open Lab Co., Ltd., 350015, Fuzhou, China.

Received: 31 December 2019 Accepted: 11 December 2020
Published online: 22 January 2021

References

1. H. Cheng, Z. Xie, L. Wu, Z. Yu, R. Li, Data prediction model in wireless sensor networks based on bidirectional LSTM. J. Wirel. Commun. Netw. **2019**, 203 (2019). https://doi.org/10.1186/s13638-019-1511-4
2. N. Liu, J. Pan, T. Nguyen, A bi-population quasi-affine transformation evolution algorithm for global optimization and its application to dynamic deployment in wireless sensor networks. J Wirel. Commun. Netw. **2019**, 175 (2019). https://doi.org/10.1186/s13638-019-1481-6
3. H. Cheng, D. Feng, X. Shi, C. Chen, Data quality analysis and cleaning strategy for wireless sensor networks. J Wirel. Commun. Netw. **2018**, 61 (2018). https://doi.org/10.1186/s13638-018-1069-6
4. W. Guo, W. Zhu, Z. Yu, J. Wang, B. Guo, A survey of task allocation: contrastive perspectives from wireless sensor networks and mobile crowdsensing. IEEE Access **7**, 78406–78420 (2019)
5. W. Fang, N. Cui, W. Chen, W. Zhang, Y. Chen, A trust-based security system for data collecting in smart city. IEEE Trans. Ind. Inf. **1**, 1 (2020). https://doi.org/10.1109/TII.2020.3006137
6. H. Cheng, Z. Su, N. Xiong, Y. Xiao, Energy-efficient node scheduling algorithms for wireless sensor networks using Markov random field model. Inf. Sci. **329**, 461–477 (2016). https://doi.org/10.1016/j.ins.2015.09.039
7. X. Zheng, W. Zheng, Y. Yang, W. Guo, V. Chang, Clustering based interest prediction in social networks. Multimed. Tools Appl. **78**, 32755–32774 (2019). https://doi.org/10.1007/s11042-018-7009-y
8. C.-H. Chen, F.-J. Hwang, H.-Y. Kung, Travel time prediction system based on data clustering for waste collection vehicles. IEICE Trans. Inf. Syst. **E102.D**(7), 1374–1383 (2019). https://doi.org/10.1587/transinf.2018EDP7299
9. X. Wu, X. Zhang, An efficient pixel clustering-based method for mining spatial sequential patterns from serial remote sensing images. Comput. Geosci. **124**, 128–139 (2019). https://doi.org/10.1016/j.cageo.2019.01.005
10. Z. He, C. Yu, Clustering stability-based evolutionary K-means. Soft Comput. **23**, 305–321 (2019). https://doi.org/10.1007/s00500-018-3280-0
11. X. Liao, L. Zhang, J. Wei, D. Yang, G. Chen, Recommending mobile microblog users via a tensor factorization based on user cluster approach. Wirel. Commun. Mobile Comput. **2018**, 11 (2018). https://doi.org/10.1155/2018/9434239
12. W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless micro-sensor networks, in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS '00), January 2000*.
13. Z. Ning, X. Hu, Z. Chen et al., A cooperative quality aware service access system for social internet of vehicles. IEEE Int. Things J. **5**(4), 2506–2517 (2018)
14. Z. Ning, F. Xia, X. Hu et al., Social-oriented adaptive transmission in opportunistic internet of smartphones. IEEE Trans. Ind. Inf. **13**(2), 810–820 (2017)
15. Z. Ning, L. Liu, F. Xia et al., CAIS: A Copy Adjustable incentive scheme in community-based socially-aware networking. IEEE Trans. Veh. Technol. **66**(4), 3406–3419 (2017)
16. X. Wang, Z. Ning, M. Zhou et al., Privacy-preserving content dissemination for vehicular social networks: challenges and solutions. IEEE Commun. Surv. Tutor. **21**(2), 1314–1345 (2019)
17. W. Fang, W. Zhang, Y. Yang, Y. Liu, W. Chen, A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution. Sci. China Inf. Sci. **60**(4), 040305 (2017)
18. W. Fang, C. Zhang, Z. Shi, Q. Zhao, L. Shan, BTRES: beta-based trust and reputation evaluation system for wireless sensor networks. J. Netw. Comput. Appl. **59**(1), 84–92 (2016)
19. Y. Chae, L.C. DiPippo, Y.L. Sun, Trust management for defending on-off attacks. IEEE Trans. Parallel Distrib. Syst. **26**(4), 1178–1191 (2015)
20. Y. Ren, V.I. Zadorozhny, V.A. Oleshchuk, F.Y. Li, A novel approach to trust management in unattended wireless sensor networks. IEEE Trans. Mob. Comput. **13**(7), 1409–1423 (2014)
21. S.A. Hussain, I. Raza, M.M. Mehdi, A cluster based energy efficient trust management mechanism for medical wireless sensor networks (MWSNs), in *2018 5th International Conference on Electrical and Electronic Engineering (ICEEE), Istanbul* (2018), pp. 433–439
22. N. Labraoui, A reliable trust management scheme in wireless sensor networks, in *2015 12th International Symposium on Programming and Systems (ISPS), Algiers* (2015), pp. 1–6.
23. F. Fang, J. Li, J. Li. A reputation management scheme based on multi-factor in WSNs, in *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), Shengyang* (2013), pp. 3843–3848
24. N. Zhou, W. Fang, W. Zhang, X. Lv, J. Huang, A novel trust management scheme for defending against on-off attack based on gaussian distribution, in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada* (2018), pp. 1806–1811.
25. A.M. Kowshalya, M.L. Valarmathi, Trust management for reliable decision making among social objects in the Social Internet of Things. IET Netw. **6**(4), 75–80 (2017)
26. X. Wu, J. Huang, J. Ling, L. Shu, BLTM: beta and LQI based trust model for wireless sensor networks. IEEE Access **7**, 43679–43690 (2019)
27. G. Han, Y. He, J. Jiang, N. Wang, M. Guizani, J.A. Ansere, A synergetic trust model based on SVM in underwater acoustic sensor networks. IEEE Trans. Veh. Technol. **68**(11), 11239–11247 (2019)

28. W. Fang, C. Zhu, W. Chen, W. Zhang, J.J.P.C. Rodrigues, BDTMS: binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network, in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol* (2018), pp. 382–387.
29. Ouafaa, E. Mustapha, K. Salah-ddine, E.H. Said, A new secure solution for clustering in wireless sensors networks based on LEACH, in *2017 International Conference on Engineering and Technology (ICET), Antalya* (2017), pp. 1–5.
30. J. Barad, B. Kadhiwala. DIST-LEACH: a deterministic key management scheme for securing cluster-based sensor networks. in *2014 International Conference on Advances in Engineering & Technology Research (ICAETR-2014), Unnao* (2014), pp. 1–5.
31. H.B. Patel, D.C. Jinwala, E-LEACH: improving the LEACH protocol for privacy preservation in secure data aggregation in Wireless Sensor Networks, in *2014 9th International Conference on Industrial and Information Systems (ICIIS), Gwalior* (2014), pp. 1–5.
32. R.K. Kodali, S.K. Gundabathula, L. Boppana, Multi level secure LEACH protocol model using NS-3, in *2014 First International Conference on Networks & Soft Computing (ICNSC2014), Guntur* (2014), pp. 198–202.
33. F. Mezrag, S. Bitam, A. Mellouk. Secure routing in cluster-based wireless sensor networks, in *GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore* (2017), pp. 1–6.
34. M. El_Saadawy, E. Shaaban, Enhancing S-LEACH security for wireless sensor networks, in *2012 IEEE International Conference on Electro/Information Technology, Indianapolis, IN* (2012), pp. 1–6.
35. Y. Zhang, L. Wei, Improving the LEACH protocol for wireless sensor networks, in *IET International Conference on Wireless Sensor Network 2010 (IET-WSN 2010), Beijing* (2010), pp. 355–359.
36. J. Wang, G. Yang, S. Chen, Y. Sun, Secure LEACH routing protocol based on low-power cluster-head selection algorithm for wireless sensor networks, in *2007 International Symposium on Intelligent Signal Processing and Communication Systems, Xiamen* (2007), pp. 341–344
37. L. Zhou, Y. Fang, Q. Wei, Y. Jin, Z. Hu, LEACH-TLC: a strategy of reducing and uniform energy consumption based on target location constraint. IET Wirel. Sens. Syst. **9**(6), 347–357 (2019)
38. K. Amirthalingam, Anuratha, Improved LEACH: a modified LEACH for wireless sensor network, in *IEEE International Conference on Advances in Computer Applications (ICACA), Coimbatore* (2016), pp. 255–258.
39. W. Fang, L. Zhang, Z. Shi, Y. Sun, L. Shan, Binomial-based trust management system in wireless sensor networks. Chin. J. Sens. Actuators **28**(5), 703–708 (2015)
40. P. Nayak, A. Devulapalli, A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime. IEEE Sens. J. **16**(1), 137–144 (2016)

Publisher's Note