Binomial Distribution Based Reputation for WSNs: A Comprehensive Survey

Zhe Wei[1] and **Shuyan Yu**[2*]
[1] School of Computer Science, Civil Aviation Flight University of China
Sichuan, 618307 China
[e-mail: findz@qq.com]
[2] Shaoxing University Yuanpei College
Shaoxing, 312000 China
[e-mail: shuyanyu1231@qq.com]
*Corresponding author: Shuyan Yu

Received June 21, 2021; revised July 30, 2021; accepted Septebmer 16, 2021; published October 31, 2021

Abstract

Most secure solutions like cryptography are software based and they are designed to mainly deal with the outside attacks for traditional networks, but such soft security is hard to be implemented in wireless sensor networks to counter the inside attacks from internal malicious nodes. To address this issue, reputation has been introduced to tackle the inside malicious nodes. Reputation is essentially a stimulating mechanism for nodes' cooperation and is employed to detect node misbehaviors and improve the trust-worthiness between individual nodes. Among the reputation models, binomial distribution based reputation has many advantages such as light weight and ease of implementation in resource-constraint sensor nodes, and accordingly researchers have proposed many insightful related methods. However, some of them either directly use the modelling results, apply the models through simple modifications, or only use the required components while ignoring the others as an integral part of the whole model, this topic still lacks a comprehensive and systematical review. Thus the motivation of this study is to provide a thorough survey concerning each detailed functional components of binomial distribution based reputation for wireless sensor networks. In addition, based on the survey results, we also argue some open research problems and suggest the directions that are worth future efforts. We believe that this study is helpful to better understanding the reputation modeling mechanism and its components for wireless sensor networks, and can further attract more related future studies.

Keywords: binomial distribution, malicious nodes, reputation, secure solution, wireless sensor networks.

This work is partially supported by the Scientific Project of CAFUC under grant nos. F2017KF02 and J2018-3, the Central University Teaching Reform Project under grant nos. E2020044 and E2021038, and Civil Aviation Professional Project under grant no. 0252109.

http://doi.org/10.3837/tiis.2021.10.017 **ISSN : 1976-7277**

1. Introduction

In wireless sensor networks, or WSNs, individual sensors are resource constraint devices with limited computing power and memory capacity, and they are usually deployed in unattended areas where adversaries could possibly physically take over a sensor and obtain the secret information stored within the sensor. However, traditional security schemes such as cryptography and authentication are mainly applied to defend against the external attacks rather than the internal ones [1]. Some studies demonstrate reputation or trust mechanism is becoming an effective approach to detect and defend against the internal attacks for WSNs [2].

Reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time [3]. In wireless sensor networks, the main characteristics of a reputation system framework are reputation expression, reputation construction, reputation updating and reputation management that is for the reputation evaluation and fusion. Generally, in wireless sensor networks, the reputation of a given node is maintained and stored by its neighbors, and in the reputation system, each node keeps (direct) reputation information about other nodes (usually within the communication range). The (direct) reputation information of each node is exchanged and shared regularly in the network, and the direct reputation information and the shared indirect reputation information from other nodes are fused by a certain algorithm to form a relatively complete reputation value about a node.

Many existing reputation systems are constructed based on statistical characteristics, such as game theory [4-7], machine learning [8-11], block chain [12-15], D-S theory [16-17], fuzzy logic [18-19], and Bayesian theorem [20-45]. These systems try to resist the selfish behavior or malicious behavior of nodes by emphasizing the cooperation between those nodes. This study focuses on the binomial distribution based reputation because it is a light-weight mechanism and energy efficient to be implemented in resource constrained individual sensors. Recently, researchers have proposed many methods to use binomial distribution based reputation modeling for WSNs. However, some either directly use the modelling results, apply the models through simple modifications, or only use the required components while ignoring the others as an integral part of the whole model. By far, this topic still lacks a comprehensive and systematical review. Thus the motivation of this study is to provide a thorough survey concerning the binomial distribution based reputation for wireless sensor networks.

The contributions and organization of this study are as follows. The determination of node behaviors will have a significant impact on the decision-making of the reputation system, and the research on node behaviors is helpful to accurately build the reputation engine. Therefore, in Sec. 2 we start from the study of node behavior classification and characteristics in WSNs, and make a more detailed analysis on node behavior classification, behavior characteristics, causes of abnormal behavior nodes, and categories of node types. Then, in Sec.3 this paper discusses the two important information sources in the reputation system, i.e., the concept of direct reputation and indirect reputation, and the different academic viewpoints of reputation fusion between them. Next, in Sec.4 this paper covers the essential requirements and main steps of reputation management, and summarizes the typical management modes in wireless sensor networks. Furthermore, in Sec.5 about the reputation modeling methods, through studying classic related literatures, this paper systematically showcases a comprehensive theoretical research and method review on the reputation model based on binomial distribution from the perspective of reputation engine, reputation fusion, and reputation aging. Lastly, according to the survey results, we argue some open research problems and suggest the directions that are worth future efforts in Sec. 6, and Sec.7 concludes this study.

2. Node Behaviors

The essence of a reputation system is to discover the abnormal behaviors of nodes in time and punish or isolate those nodes from the system so that the damage caused can be minimized. In [29], the behaviors of nodes in wireless sensor networks are categorized into data perception and data communication, and the corresponding abnormal behaviors are divided into false data behavior and bad communication behavior. The causes of false data behaviors can be attributed to the following three aspects:

1) Due to the destruction of the node, energy exhaustion, or the failure of sensing components and other components, i.e., the false data is caused by the failure of the node itself;

2) Due to the long-term exposure of the node to the outside, the influence of the surrounding environment, or the interference of the channel signal;

3) Due to the capture of the node and failure of communication to the other nodes.

There are two main reasons for bad communication behaviors:

1) The behavior of the node itself is selfish. For the sake of saving its own energy, the node does not forward the data or selectively forwards part of the data;

2) The behavior of the node itself is malicious. When the node forwards the data, it injects false information or routes the data to other paths intentionally.

Based on the observation of node behaviors, Yang et al. [46] divide the node types into three categories: legitimate node, selfish node, and malicious node.

1) Legitimate node: a legitimate node or legal node can correctly deliver the received data packet to the next node on the premise of ensuring the integrity of the transmitted data packet. The legitimate nodes are to maintain the normal operation of the network;

2) Selfish node: a selfish node discards the received data packets in order to reduce its own energy loss or save its own computing resources, which makes these data packets cannot reach the next node. The selfish behavior of nodes will reduce the reliability of the network.

3) Malicious node: the main purpose of a malicious node is to attack and destroy the network, which reduces the integrity of the network and poses a great threat to the network security. For example, during the routing request, malicious nodes provide the wrong routing information or intentionally pass the data packets to other nodes outside the right path; during the data packet transmission, they tamper with the data packet to be submitted or inject the wrong data into the data packet. Malicious nodes can also collude with other malicious ones to jointly attack a node, such as reducing the reputation of this node.

In addition, according to the behaving characteristics of nodes, the behaviors of nodes are further divided into the following five categories:

1) Continuous malicious behaving node. Malicious behaviors of these nodes are frequent, such as always injecting or modifying packets received and sending them to other nodes;

2) Intermittent malicious behaving node. Malicious behaviors of these node are sometimes present while absent in other times;

3) Continuous selfish behaving node. Continuous selfish behaving nodes generally do not inject or modify the data packets they receive, but for some reasons such as saving their own resources, they will continuously reject the services requested by other nodes or often discard the data packets they receive;

4) Intermittent selfish behaving node. Compared with continuous selfish behaving nodes, intermittent selfish behaving nodes will intermittently reject the services requested by other nodes or sometimes discard the data packets they receive;

5) Intermittent friendly behaving node. An intermittent friendly behaving node sometimes discards the received data packets due to temporary failures such as communication errors;

Generally, if the behavior of a node is always good, its reputation value will continue to add up, and vice versa. For example, in a process of a routing information request, when *A* successfully responds to the routing information request from *B*, *B* will correspondingly improve the reputation value of *A* based on the behavior result of *A*. Nodes with good behaviors (nodes with high reputation value) will also be given *preferential treatment* in the network. For example, node *E* has four neighbor nodes: *A*, *B*, *C*, and *D*. These neighbor nodes have different reputation values, and *E* usually chooses *D* which has the highest reputation value to cooperate with in a certain task.

3. Direct and Indirect Reputation

Reputation modeling is to express mathematically how one node in the network judges or scores the results of another node's behavior. In wireless sensor networks, the information needed for reputation modeling mainly comes from two aspects: direct reputation which comes from the direct observation of nodes themselves; indirect reputation that comes from the direct observation of neighboring nodes.

Although direct observation is simple and intuitive, it is also subjective and one-sided. Therefore, in addition to direct observation, it is necessary to integrate, analyze and process the direct observation results from other nodes, that is, to form indirect observation results. Reputation information obtained through indirect observation is also called second-hand reputation information. It can be seen that the establishment of direct reputation does not need the participation of the third parties, while the establishment of indirect reputation is completed with the participation of the third parties.

In a system with direct and indirect reputation, all nodes need to broadcast their own direct reputation information tables about the third-party nodes to their neighbors regularly. For example, when node *A* receives the direct reputation about node *C* from node *B*, *A* will use a certain algorithm to fuse its own direct reputation about *C* with the direct reputation about *C* from *B* so as to compute the comprehensive reputation of *C*.

However, there are some controversies about the advantages and disadvantages of indirect reputation information. In wireless sensor networks, the sharing of indirect reputation information often means extra communication overhead. This is because the purpose of indirect reputation sharing is to make the reputation information of a node public. Although it helps the system to shorten the identification time of abnormal behaving nodes, the maintenance and transmission of indirect reputation will not only lead to the extra overhead of a single node, but also brings extra cost to the whole network system [47]. Similar views can be found in [48] that the indirect reputation information obtained by other nodes cannot bring accuracy and reliability to the reputation computing, instead it makes the reputation system vulnerable to external attacks, such as bad mouth attack and ballot stuffing attack [49].

Besides, the reputation of normal nodes can be improved or reduced by malicious nodes colluding with each other at any time [50]. Therefore, in [51], node reputation only comes from direct reputation, and indirect reputation exchange is not allowed. Nevertheless, some literatures such as [20-21] support the combination of direct reputation and indirect reputation so as to improve the objectivity of the reputation.

Although the combination of direct reputation information and indirect reputation information can more comprehensively measure the reputation of a node, the introduction of indirect reputation will also bring certain risks to the whole system. We believe that the indirect reputation should be used, but it is necessary to find a balance between the two, so that both can better serve the reputation system. Related methods and how to implement the indirect

reputation is presented in Section 5.

4. Reputation Management

Reputation management usually refers to the management of reputation source and reputation evaluation in a reputation system. A reputation system can be divided into two main types: centralized and distributed. The structure of a reputation system determines how the reputation evaluation is transferred and exchanged among system participants.

4.1 Requirements

In the reputation system, the nodes participating in a certain task in the network evaluate the reputation of their cooperative nodes and gradually form a trust relationship. Therefore, reputation management is a framework to establish and manage the trust relationship between these nodes [52], further, the reputation management should meet the following requirements:

1) Decentralized management mode. Each node in the network is an autonomous entity, and it should have the ability to make decisions independently in terms of reputation management and configuration. The management should be based on P2P or Ad hoc mode, and the reliance on centralized management mode should be avoided;

2) Simple usage and low operation overhead. The reputation management model should be oriented to end users, so the management mode should be as simple as possible, and the parameters in the management model can be obtained by mathematical model, rather than by subjective or abstract way of human intervention. In addition, the operation requirements of the reputation model should be as low as possible so that it can be used in most network nodes, and nodes can adopt the reputation management model at any time, in any place and any network environment.

3) Management should be dynamic and cooperative. The establishment and maintenance of the reputation management model should be dynamic and change with time. Reputation information should be shared by different nodes or entities locally, and the whole network should be managed by the mutual cooperation of these entities;

4) Establishment of untrusted model and granularity of trust evaluation. In the reputation management, untrusted nodes and trusted nodes are equally important, and the management should be able to effectively identify malicious nodes and avoid any transactions or cooperation with them. In addition, granularity also makes the reputation evaluation of nodes more accurate than pure numerical data.

5) Management should have a certain anti-attack ability. Because the nodes in the network are often exposed outdoors, they are vulnerable to a variety of internal and external attacks, so the reputation management system should have a certain anti-attack ability, make a timely response to the attack and have the corresponding countermeasures.

4.2 Main Steps

In wireless sensor networks, the reputation management system plays a very important role in the decision-making, and another main function is to solve the uncertainty. Uncertainty refers to the uncertainty of the results in a certain environment. Uncertainty mainly comes from the following aspects: asymmetric information, that is, one party does not have all the information about the other party; speculative, namely, the two parties involved have different purposes. Due to the existence of uncertainty, a node cannot determine the behavior of the other party before the transaction or cooperation, especially when the partner is a potential malicious node, it will have a certain negative impact on the cooperation initiator. Therefore, uncertainty is one

of the problems that must be solved in wireless sensor networks, the reputation mechanism can help nodes to avoid the above problems and choose nodes with good reputation to cooperate with [53-54], and the reputation management in wireless sensor networks can generally follow the steps:

1) In addition to a node's own direct observation, that node can ask its nearby nodes about the reputation information of the third-party node, that is, reputation can be obtained indirectly;

2) Fuse the direct reputation and indirect reputation so as to compute the reputation of the node to be evaluated;

3) Select the node with the highest reputation among all nodes and request services from it;

4) After the service is provided, reputation of the node is evaluated according to the service quality or user satisfaction, and the reputation is then updated accordingly.

5. Binomial Distribution Based Reputation

Among many theoretical methods of reputation modeling, statistical methods such as Beta distribution, Poisson distribution and Gaussian distribution have been widely concerned by scholars. Among these methods, binomial distribution is widely used to build reputation. This method is simple and has strong statistical basis in theory. In particular, this method only needs two parameters which can represent the number of positive evaluations and negative evaluations respectively in practical applications, making it very suitable for reputation construction of wireless sensor networks. More importantly, this method is light-weight suitable for resource constraint sensor nodes. Literatures such as [20−45] and [55-69] use this reputation method which generally consists of three components, i.e., reputation engine, reputation fusion, and reputation aging.

5.1 Reputation Engine

Before describing the reputation engine, the definition of Beta distribution function is given by

$$Beta(\alpha,\beta)=\int_0^1 v^{\alpha-1}(1-v)^{\beta-1}dv \tag{1}$$

where (α,β) is called the shape parameter of Beta distribution. The probability density function of Beta distribution is defined by

$$f(p\mid\alpha,\beta)=\frac{p^{\alpha-1}(1-p)^{\beta-1}}{Beta(\alpha,\beta)} \tag{2}$$

where $0\le p\le 1$is the probability variable. Traditionally, Beta probability density function $f(p\mid\alpha,\beta)$ is usually described and expressed by gamma function Γ, (1) is redefined by

$$f(p\mid a,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \tag{3}$$

where $\Gamma(n)=n!$. The mathematical expectation of Beta distribution is defined by

$$E(p)=\frac{\alpha}{\alpha+\beta} \tag{4}$$

In a wireless sensor network, for example, assume that there are n nodes $(N_1,N_2,...N_n)$. After being deployed, any pair of nodes $(N_i,N_j)\subseteq N$ can communicate directly with each

other. Suppose that under a certain monitoring mechanism, the outcome of a transaction (such as data transmission, routing information request and response, etc.) between nodes only has two states: success or failure, cooperation or non-cooperation. Now N_1 wants to request routing information from its neighbor nodes $(N_2, N_3, ..., N_n)$, and the probability that these neighbor nodes will respond is $(p_2, p_3, ..., p_n)$ respectively. In practice, it is impossible for N_1 to determine the specific value of $(p_2, p_3, ..., p_n)$ in advance, but p_i can be regarded as the probability of success of random test in binomial distribution. In addition, according to Casella [70], for any distribution, there is a natural prior distribution family called conjugate family. In Bayesian theory, Beta distribution can be regarded as the prior distribution of binomial distribution, and p_i can be obtained according to (4) which it is defined by

$$E(p_i) = \frac{\alpha_i}{\alpha_i + \beta_i} \tag{5}$$

In applications, N_1 can estimate p_i by recording N_i's response times α_i and non-response times β_i in previous routing information requests. In (5), $E(p_i)$ can usually be regarded as the reputation value of node N_i in some activities such as routing information response, while α_i and β_i can be regarded as the number of cooperation (positive evaluation) and non-cooperation (negative evaluation) in these activities respectively.

After N_1 selects N_i for cooperation, the next step is to update the reputation of N_i. In Bayesian statistical inference, the posterior distribution of binomial distribution is also Beta distribution. Jøsang et al. [60] use the following method to update the reputation: considering the number of responses α_i and the number of non−responses β_i recorded by node N_1 about N_i in the past routing information responses, the probability density function that node N_i can respond to the next routing information request is as defined by

$$f(p' \mid a+1, \beta+1) = \frac{\Gamma(\alpha+\beta+2)}{\Gamma(\alpha+1)\Gamma(\beta+1)} p'^{(\alpha-1)}(1-p')^{\beta-1} \tag{6}$$

and its mathematical expectation is defined by

$$E(p') = \frac{\alpha+1}{\alpha+\beta+2} \tag{7}$$

Many literatures such as [26-29, 55-69] used the above method to update the reputation. The following presents the detail process which can be further referred in RFSN.

1) Define the node transaction content and the evaluation result. RFSN defines a transaction as two nodes in the network participating in and completing a task that requires mutual cooperation, such as data packet switching and transmission. After the completion of each task, both sides will evaluate the other party according to the completion of the task. RFSN defines the evaluation results as *cooperative* and *non- cooperative*.

2) Compute the node reputation θ. Before performing a task, entities usually instinctively choose other entities with good reputation to cooperate with. In RFSN, reputation θ is used to

represent the probability that node N_i can cooperate when other nodes send data packet delivery requests to it. The binomial distribution in statistics meets the modeling conditions when only the node behavior is considered to be cooperative or non-cooperative. Like (6), in RFSN, Beta distribution is used as the prior distribution function of binomial distribution, and binomial distribution function $f(\theta)$ is used to express θ, i.e.

$$f(\theta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \tag{8}$$

where $\theta\in[0,1],\alpha,\beta>0$. In the process of solving θ, similar to (7), the method of calculating the mathematical expectation is used, namely

$$E(\theta)=\frac{\alpha}{\alpha+\beta} \tag{9}$$

3) Compute node transaction evaluation Y. After computing the value of θ, it can be regarded as the success probability of Bernoulli test, and let $Y\in[0,1]$ represent the evaluation of node N_i by other nodes when the data packet is transferred. According to the definition of binomial distribution, Y is defined by

$$P(Y\mid\theta)=\theta^{Y}(1-\theta)^{1-Y} \tag{10}$$

4) Compute the posterior distribution of θ (reputation update). After the transaction, since the posterior distribution of binomial distribution is still Beta distribution, the posterior probability of θ is defined by

$$P(\theta\,|\,Y)=\frac{P(Y\,|\,\theta)P(\theta)}{\int P(Y\,|\,\theta)P(\theta)d\theta}\sim Beta(\alpha+Y,\beta+1-Y) \tag{11}$$

Equation (11) shows that the posterior probability $P(\theta\mid Y)$ follows the Beta distribution with parameter $(\alpha+Y,\beta+1-Y)$. It can be seen that when the data packet transmission is completed, the two reputation parameters of node N_i turn into

$$\begin{cases}\alpha^{new}=\alpha^{old}+Y\\ \beta^{new}=\beta^{old}+1-Y\end{cases} \tag{12}$$

Then the mathematical expectation of N_i's reputation θ after completing the task is

$$E(\theta)=\frac{\alpha^{new}+Y}{\alpha^{new}+Y+\beta^{new}+1-Y} \tag{13}$$

In the case of n times of the same task and with evaluation $Y_1,Y_2,...,Y_n\in[0,1]$, according to RFSN, the posterior distribution of θ of node N_i is still beta distribution, and its two reputation parameters become

$$\begin{cases}\alpha^{new}=\alpha^{old}+n\overline{Y}\\ \beta^{new}=\beta^{old}+n(1-\overline{Y})\end{cases} \tag{14}$$

and the reputation θ is updated to

$$E(\theta)=\frac{\alpha^{old}+n\overline{Y}}{\alpha^{old}+n\overline{Y}+\beta^{old}+n(1-\overline{Y})} \tag{15}$$

From the above computing principle of reputation engine, it can be seen that the reputation calculation is based on the past behavior of the supervised node directly observed by the supervising node through a certain supervising or detecting mechanism. For example, Ozdemir [61] sets the network card of node to be promiscuous mode for direct reputation observation whereby node *A* observes the number of the correct delivery, discarding or malicious modification of the data packets by node *B*. Node *A* inputs these observed results as shape parameters into the reputation model and obtains the reputation parameters of node *B* according to the mathematical expectation of the reputation model.

On computing the direct reputation, Liu et al. [46] use a mechanism called moving mechanism to deal with the malicious behavior of some nodes. If the malicious behavior of the node exceeds the specified threshold, the size of the moving window will be halved, and the reputation value of the node will be dropped rapidly, which means that the malicious node will be detected by the system quickly. If the malicious node attempts to change its behavior, i.e. its behavior becomes friendly, the size of the moving window will be increased, which indicates that the malicious node can redeem its reputation within a certain period of time. Hence the moving mechanism can reduce the impact of malicious behavior of nodes on the system to a certain extent, but for the selfish behavior of nodes, [46] does not specifically discuss how to deal with them.

In addition, the size of moving window also affects the result of reputation computing. If the window is too small, the system will be greatly affected by the node behavior, which is not suitable for the wireless sensor networks that transmit data through wireless mode and sometimes suffer from packet errors related to the transmission medium. If the window is too large, the system will react slowly to the behavior of nodes, which is not conducive to detecting malicious nodes in time. Yet the selection of the window size is not discussed in detail.

5.2 Reputation Fusion

Reputation system is easy to be cheated by false reputation information (malicious bad comments or false praise). Drawbacks could exist by using only direct reputation obtained by direct observation, such as subjectivity, incomprehensibility, and not making full use of all available indirect reputation information. In addition, due to the data packet conflict or other errors related to the transmission medium, the direct monitoring mode of direct reputation will occasionally produce wrong observation results and inaccurate direct reputation information.

Consider the following situation: it is believed that the higher the reputation of a node is, the more likely the node is to be selected by other nodes as the partner of a task; assume that the reputation of node *A* is 0.65 and that of node *B* is 0.651, if the node with the highest reputation is selected according to the general principle, *B* is naturally selected; however, the reputation difference between node *A* and node *B* is only 0.001, which can be ignored to a certain extent. Because the reputation difference between them is so small, no matter whom is selected, there may be little difference in the result of cooperation. So it is unfair not to choose *A*. Intuition tells us that in addition to using direct reputation information, indirect reputation information from third parties is also very important.

In fact, the convergence time of a reputation system using only direct reputation is very long, so it is necessary to add indirect reputation to confirm the direct reputation information [21]. In addition, the direct reputation is based on the subjective observation of the observed

object, and the indirect reputation from all the third parties can modify the direct reputation, making the direct reputation more accurate and objective. However, the two kinds of reputation should be integrated in a more reasonable way, otherwise malicious nodes through colluding with each other launch attacks on a node with good reputation, and over time, more good behaving nodes will become victims [61].

Therefore, it is necessary for the wireless sensor network node to evaluate the reputation information of other nodes directly observed by itself, and then share the reputation information with other nodes in the network. In [71], this shared reputation information is called soft data. In the reputation system, soft data needs to be properly processed before it can be integrated into the reputation system. However, different reputation systems use different methods to solve the problem of what kind of indirect reputation information or soft data can be shared. For example, some reputation system prohibits the spread and sharing of negative reputation information, so as to reduce the joint attacks launched by malicious nodes. West [71] proposes a method of sharing all indirect reputation information. Momani et al. [71] use expert opinion method [72-73] (the opinion provided by the knowledge source is called expert opinion, which is a method of combining soft data and hard data according to the rule of probability) to further verify the effectiveness of the indirect reputation from each node.

In order to avoid false indirect reputation information fusion, Rackley [74] calculates whether the Euclidean distance between direct reputation information and indirect reputation information is less than the given value. Once satisfied, the indirect reputation and the direct reputation can be fused.

While in [68], node N_i in the network not only keeps its own direct reputation information about its neighbor nodes such as N_j, but also exchanges reputation information with other nodes in the network. In addition, when certain conditions are met, it also receives indirect reputation information from other nodes such as N_k. Therefore, the reputation fusion of nodes in the network includes two aspects:

1) Self-direct reputation information fusion. RDAS [24] uses the reputation calculation method similar to (12), but uses the following method when updating reputation.

$$\begin{cases} \alpha_{i,j}' = u\alpha_{i,j} + s \\ \beta_{i,j}' = u\beta_{i,j} + (1-s) \end{cases} \tag{16}$$

where $(\alpha_{i,j}, \beta_{i,j})$ is the past reputation parameter of node N_j held by node N_i, $(\alpha_{i,j}', \beta_{i,j}')$ is the current reputation parameter to be computed, and u is the discount factor aiming to weaken the influence of past reputation parameter. When N_j and N_i are judged to cooperate in a certain transaction $s = 1$, otherwise $s = 0$.

2) The direct reputation is fused with the direct reputation from other nodes. For example, when node N_i fuses the reputation parameter about N_j from node N_k, it does not simply use the method of adding reputation parameters, but first checks the deviation of two groups of reputation parameters whether it satisfies

$$| E(Beta(\alpha_{i,j}, \beta_{i,j})) - E(Beta(\alpha_{k,j}, \beta_{k,j})) | \le D \tag{17}$$

where $D > 0$ is the deviation and is a constant. Only when the above condition is satisfied can N_i fuse the reputation about N_j from node N_k. The weighted addition method is applied as:

$$E'(Beta(\alpha_{i,j}, \beta_{i,j})) = E(Beta(\alpha_{i,j}, \beta_{i,j})) + wE(Beta(\alpha_{k,j}, \beta_{k,j})) \tag{18}$$

where $w > 0$ is the weight. RDAS also uses a similar reputation updating method. Lastly, the behavior of node N_k is determined according to the fused reputation information. The results

are as follows.

$$\begin{cases} Normal, if\ \ E'(Beta(\alpha_{i,j},\beta_{i,j})) \geq T \\ Malicious, if\ \ E'(Beta(\alpha_{i,j},\beta_{i,j})) < T \end{cases} \tag{19}$$

where $T > 0$ is the given reputation threshold.

Similarly, to effectively deal with malicious behavior from high reputation nodes, I-BRSN [75] introduces the credibility of the third-party node and calculates it in the following way:

$$\begin{cases} \alpha_{ik} = \alpha_{ik} + w, \quad \left|C_{ij} - C_{kj}\right| = \left|\dfrac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} - \dfrac{\alpha_{kj}+1}{\alpha_{kj}+\beta_{kj}+2}\right| \leq \theta \quad \theta \in [0,1) \\ \beta_{ik} = \beta_{ik} + w, \quad \left|C_{ij} - C_{kj}\right| = \left|\dfrac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} - \dfrac{\alpha_{kj}+1}{\alpha_{kj}+\beta_{kj}+2}\right| > \theta \quad \theta \in [0,1) \end{cases} \tag{20}$$

where α_{ij} and β_{ik} are the reputation parameters of node *k* held by node *i*, w is a constant, C_{ij} and C_{kj} are the credibility of node *j* held by node *i* and node *k* respectively. When the absolute value of the difference between C_{ij} and C_{kj} is greater than the predefined threshold value θ, it means that node *i* and node *k* have a large deviation about the reputation of node *j*, then node *k* is considered to deliberately improve or reduce the reputation of node *j*, and the penalty measure is taken as $\beta_{ik}^{IR} = \beta_{ik}^{IR} + w$, otherwise $\alpha_{ik}^{IR} = \alpha_{ik}^{IR} + w$.

Jøsang et al. [60] use two methods of reputation information fusion. The first method uses the direct addition of reputation parameters, and the second one uses the *BD* (belief discounting) for reputation fusion. Suppose there are three nodes N_1, N_2 and N_3 in the network. In a certain transaction, the reputation parameters of N_2 and N_3 held by N_1 are $(\alpha_{1,2},\beta_{1,2})$ and $(\alpha_{1,3},\beta_{1,3})$ respectively, while the reputation parameters of N_3 held by N_2 in this transaction are $(\alpha_{2,3},\beta_{2,3})$.

In the first fusion method, the reputation parameters about N_3 held by N_1 are fused by the reputation parameters about N_3 held by N_2, and the results are as follows:

$$\begin{cases} \alpha_{1,3}^2 = \alpha_{1,3} + \alpha_{2,3} \\ \beta_{1,3}^2 = \beta_{1,3} + \beta_{2,3} \end{cases} \tag{21}$$

Although using (21) for reputation fusion calculation is relatively simple, but the reliability of reputation about node N_3 from node N_2 is still worth further discussion, which also makes the reputation system vulnerable to attacks like bad mouth attack and ballot stuffing attack.

In ballot stuffing, malicious entities usually collude to give a positive evaluation to an entity, which makes the reputation of the latter improve rapidly in a short time, and also makes the latter qualified (for malicious purposes) to engage in a task. On the contrary, in the bad mouth attack, malicious entities collude with each other to give a negative evaluation to an entity, which makes the reputation of the latter decrease rapidly in a short time, and eventually leads to the latter not qualified to participate in network tasks or isolated by the network [49].

The second method uses Dempster Shafer [16] theory to deal with reputation fusion, or *BD* (belief discounting) method. *BD* method uses opinion to describe the credibility of a statement. The opinion is a triple. For example, the opinion of node X to node Y is expressed as

$$O_Y^X = (b_Y^X, d_Y^X, u_Y^X) \tag{22}$$

where $b_Y^X + d_Y^X + u_Y^X = 1, b_Y^X, d_Y^X, u_Y^X \in [0,1]$. b_Y^X (*belief*) and d_Y^X (*disbelief*) represent the probability that the statement made by node X to node Y is correct or not, while u_Y^X (*uncertainty*) represents the uncertain degree that the statement made by node X to node Y is correct or not.

Let node Y 's opinion on node T be $O_T^Y = (b_T^Y, d_T^Y, u_T^Y)$, then node X 's opinion on node T through Y is $O_T^{X:Y} = (b_T^{X:Y}, d_T^{X:Y}, u_T^{X:Y})$, and according to [60], $b_T^{X:Y}, d_T^{X:Y}, u_T^{X:Y}$ satisfies

$$b_T^{X:Y} = b_Y^X b_T^Y, d_T^{X:Y} = d_Y^X d_T^Y, u_T^{X:Y} = d_Y^X + u_Y^X + b_Y^X u_T^Y \tag{23}$$

Map the above equation to Beta reputation model, the following relationship is obtained

$$b = \frac{\alpha}{\alpha+\beta+2}, d = \frac{\beta}{\alpha+\beta+2}, u = \frac{2}{\alpha+\beta+2} \tag{24}$$

Substitute (24) into (23), the following relationship is obtained

$$\begin{cases} \alpha_{1,3}^2 = \alpha_{1,3} + \dfrac{2\alpha_{1,2}\alpha_{2,3}}{(\beta_{1,2}+2)(\alpha_{2,3}+\beta_{2,3}+2)+2\alpha_{1,2}} \\ \beta_{1,3}^2 = \beta_{1,3} + \dfrac{2\alpha_{1,2}\beta_{2,3}}{(\beta_{1,2}+2)(\alpha_{2,3}+\beta_{2,3}+2)+2\alpha_{1,2}} \end{cases} \tag{25}$$

In [21], the reputation fusion method is similar to that in [60], but it is slightly different in expression. In [21], the reputation fusion is expressed as

$$\begin{cases} \alpha_j^{new} = \alpha_j + \dfrac{2\alpha_k\alpha_j^k}{(\beta_k+2)(\alpha_j^k+\beta_j^k+2)+2\alpha_k} \\ \beta_j^{new} = \beta_j + \dfrac{2\alpha_k\beta_j^k}{(\beta_k+2)(\alpha_j^k+\beta_j^k+2)+2\alpha_k} \end{cases} \tag{26}$$

where (α_j, β_j) and (α_k, β_k) represent the reputation parameters of node j and k held by node i respectively, and (α_j^k, β_j^k) represents the reputation parameters of node j held by node k. $(\alpha_j^{new}, \beta_j^{new})$ is the final result of reputation fusion. Perez-Toro et al. [24] combine the reputation fusion methods used in [69] and [60], and compute the reputation fusion as follows

$$\begin{cases} \alpha_{i,j}^{new} = u\alpha_{i,j} + r_{i,j} + \sum_{k\in N} D(\alpha_{k,j}) \\ \beta_{i,j}^{new} = u\beta_{i,j} + s_{i,j} + \sum_{k\in N} D(\beta_{k,j}) \end{cases} \tag{27}$$

where $(r_{i,j}, s_{i,j})$ is the increment of reputation parameter, μ is similar to that in (16), and $\sum_{k\in N} D(r_{k,j})$ and $\sum_{k\in N} D(s_{k,j})$ are defined by

$$\sum_{k\in N} D(\alpha_{k,j}) = \sum_{k\in N} \frac{2\alpha_{i,k}\alpha_{k,j}}{(\beta_{i,k}+2)(\alpha_{k,j}+\beta_{k,j}+2)+2\alpha_{i,k}} \tag{28}$$

$$\sum_{k\in N} D(\beta_{k,j}) = \sum_{k\in N} \frac{2\alpha_{i,k}\beta_{k,j}}{(\beta_{i,k}+2)(\alpha_{k,j}+\beta_{k,j}+2)+2\alpha_{i,k}} \tag{29}$$

where k is any third-party node and N is the set of nodes except node i and j.

In addition, to avoid the malicious reputation evaluation from the third-party node, Yin et al. [75] mainly adopt direct reputation supplemented by the indirect reputation during the reputation fusion. The proposed method is shown as follows.

$$\begin{cases} \alpha_{ij\oplus i\wedge j} = \omega_1\alpha_{ij} + \omega_2\alpha^k_{i\wedge j} \\ \beta_{ij\oplus i\wedge j} = \omega_1\beta_{ij} + \omega_2\beta^k_{i\wedge j} \end{cases} \tag{30}$$

where ω_1 and ω_2 are the corresponding weights and $\omega_1+\omega_2=1, \omega_1>\omega_2$, the calculation of $\alpha^k_{i\wedge j}$ and $\beta^k_{i\wedge j}$ is similar to that of (27).

Further, Zhou et al. [38] use the entropy theory to assign each reputation source node with different weights, the entropy of each reputation R^i is defined by

$$H(R^i) = -R^i \log_2 R^i - (1-R^i)\log_2(1-R^i) \tag{31}$$

and each related weight is defined by

$$w_i = (1-\frac{H(R^i)}{\log_2 R^i}) / \sum_{i=1}^{n} 1-\frac{H(R^i)}{\log_2 R^i} \tag{32}$$

For the purpose of attacking normal nodes, the reputation evaluation of normal nodes by malicious nodes will usually deviate from the actual reputation, which can be identified by the entropy. However, due to its computing complexity, the entropy should be used advisably.

5.3 Reputation Aging

For reputation fusion, the behavior of nodes will change with time. For example, some nodes will maintain good reputation for a period of time and start malicious behavior in the following time. Therefore, the historical reputation parameter cannot accurately measure the current reputation situation. In addition, in order to hide their malicious behavior and not be found by other nodes, malicious nodes tend to maintain good behavior at the beginning, and then launch malicious attacks when the reputation accumulates to a high reputation.

To reduce the negative impact of the above problems on the system, many reputation systems adopt the reputation aging method as a coping strategy, and some literatures also call it reputation decay. The basic idea of reputation aging is that the historical reputation parameter is usually given a smaller weight when the reputation at different times is added, and a forgetting factor *FF* is introduced in the process of historical reputation information processing, which is a constant with value less than 1 and greater than 0. In order to avoid the problem that malicious nodes launch attacks when their reputation become higher, their reputation is usually weakened by multiplying with the forgetting factor. In [60], the historical reputation fusion parameters of node j held by node i through node k is defined by

$$\begin{cases} \alpha_{i,j} = \sum_{k=1}^{n} \alpha^k_{i,j} \\ \beta_{i,j} = \sum_{k=1}^{n} \beta^k_{i,j} \end{cases} \tag{33}$$

After introducing the forgetting factor $0 \le \xi \le 1$, (33) is rewritten as

$$\begin{cases} \alpha'_{i,j} = \sum_{k=1}^{n} \alpha_{i,j}^{k} \xi^{n-k} \\ \beta'_{i,j} = \sum_{k=1}^{n} \beta_{i,j}^{k} \xi^{n-k} \end{cases} \tag{34}$$

It can be seen that in (34), the weight given by the historical reputation parameter will be smaller and smaller with the change of time, while the newer the reputation parameter is in time, the larger the weight is.

Similar to [60], in [21], the aging factor $0 \le \omega \le 1$ is used as follows

$$\begin{cases} \alpha_i^{new} = \omega \alpha_i \\ \beta_i^{new} = \omega \beta_i \end{cases} \tag{35}$$

How to select the value of $0 \le \omega \le 1$ is relatively complex. In [21], the selection of aging factor is carried out by comparing credit system with and without the aging factor.

Similarly, Yin et al. [75] define the process of reputation aging by

$$\begin{cases} \alpha_{ij \oplus i \wedge j}(t+1) = \eta * \alpha_{ij \oplus i \wedge j}(t) + \alpha_{ij \oplus i \wedge j}(\Delta t) \\ \beta_{ij \oplus i \wedge j}(t+1) = \eta * \beta_{ij \oplus i \wedge j}(t) + \beta_{ij \oplus i \wedge j}(\Delta t) \end{cases} \tag{36}$$

where $\eta \in (0,1)$ is the forgetting factor, $\alpha_{ij \oplus i \wedge j}(t)$ and $\beta_{ij \oplus i \wedge j}(t)$ represent the reputation parameters before time $t+1$, $\alpha_{ij \oplus i \wedge j}(\Delta t)$ and $\beta_{ij \oplus i \wedge j}(\Delta t)$ represent the reputation parameters between time $t+1$ and t, i.e. the reputation parameters of the latest period.

Then the final reputation (direct and indirect) of node i about node j is defined as:

$$\begin{aligned} C_{ij}(t+1) &= E(Beta(\alpha_{ij \oplus i \wedge j}(t+1)+1, \beta_{ij \oplus i \wedge j}(t+1))) \\ &= \frac{\alpha_{ij \oplus i \wedge j}(t+1)}{\alpha_{ij \oplus i \wedge j}(t+1) + \beta_{ij \oplus i \wedge j}(t+1) + 2} \end{aligned} \tag{37}$$

When $C_{ij}(t+1)$ is less than the specified threshold, node i considers j illegal or malicious.

In [38], a sliding window with *m* time slots and an adaptive forgetting factor θ_l are introduced and defined as

$$\theta_l = 1 - D^l, l = 1, 2, ..., m \tag{38}$$

where D^l is the direct reputation of the *lth* time slot. It indicates that the good or malicious behavior will be stored for a relatively longer time. The two reputation parameters are redefined by

$$\begin{cases} \alpha_{i,j} = \sum_{l=1}^{m} \alpha_{i,j}^{l} \theta_l^{m-l} \\ \beta_{i,j} = \sum_{l=1}^{n} \beta_{i,j}^{l} \theta_l^{m-l} \end{cases} \tag{39}$$

Based on the above study and analysis, these three components are essential for the binomial reputation to work normally. But among the related literatures, some merely use the required components while ignoring the others as an integral part of the whole. For example, regarding the reputation fusion, some literatures such as [21,24,26,29,35,36] use both direct

reputation and indirect reputation, while others like [30,31,33,41,42,43] only apply direct reputation. For another example, as is shown in **Table 1,** on the reputation aging, among the literatures that apply direct reputation and/or indirect reputation, only a few of them such as [21,24,25,33] use the reputation aging, while other literatures ignore it for no reason. Besides, by using the concept of binomial reputation, energy reputation [36,37], communication reputation [25,34,35,36,37], and data reputation like [30,34, 41,42,59] and so on are introduced so as to save individual node energy and ensure the reliable communication and data transmission. Further, penalty and reward mechanisms [43], light computational complexity such as [21,24,26,27], and energy issues like [43,44,76] and so on are also considered in order to stimulate node cooperation, avoid running complex algorithms, and balance the energy consumed in the network. However, few of these related literatures take the reputation redemption, adaptive reputation threshold, and adaptive forgetting factor into consideration, which is worthy of future study.

Table 1. Functional components under binomial reputation

Components	Related Works
Direct Reputation	[21][24][25][26][27][28][29][30][31][33][34][35][36][37][38][39][40] [41][42][43][44][55][56][58][59][60][61][63][64][65][66][67][76]
Indirect Reputation	[21][24][26][27][29][34][35][36][37][38][39][40][55][56][58][59][60] [61][64][65]
Reputation Aging	[21][24][25][33][35][37][39][60][61][64]
Energy Reputation	[36][37]
Communication Reputation	[25][34][35][36][37]
Data Reputation	[21][26][30][34][36][37][41][42][59]
Reputation Redemption	N/A
Penalty &Reward Consideration	[43]
Light Computational Complexity	[21][24][26][27][28][30][31][33][34][35][37][39][40][56][67][76]
Adaptive Reputation Threshold	N/A
Adaptive Forgetting Factor	N/A
Energy Consideration	[21][24][27][28][36][37][38][43][44][76]

One of the advantages of binomial distribution based reputation, or binomial reputation is its stimulating effect on the node's cooperation. Each node has to participate in a certain transaction so as to maintain its reputation. Once a node loses its reputation, it may not receive certain service from other nodes, or it could not be reputation-qualified to provide certain service for others. Accordingly, as is presented in **Table 2**, secure solutions are proposed for WSNs from the aspects of routing [25,27,28,44,58], packet delivering [25,26,34,61], data aggregation [21,24,26,27,28,44,61], and node selection [24,58,61,66] so that trust or reputation qualified nodes can be selected to fulfill these tasks. Further, a malicious node may accumulate its reputation before launching a certain attack, a malicious node may even switch between good behaviors and bad ones so as to launch attacks without being detected, and some malicious nodes give good reputation to each other and then collusively give bad reputation to a third party node. By carefully designing the binomial reputation with appropriate mechanisms, attack countermeasures, listed in **Table 2** against bad mouthing attack, on-off attack, conflicting behavior attack and so on, can be properly addressed or mitigated.

Table 2. Typical secure solutions and attack countermeasures under binomial reputation

Secure Issues &Attacks	Solutions & Countermeasures
Secure Routing	[25][27][28][44][58]
Secure Packet Delivering	[25][26][34][61]
Secure Data Aggregation	[21][24][26][27][28][44][61]
Secure Node Selection	[24][58][61][66]
Spoofed Data Attack	[25][26][31][38][67]
Bad Mouthing Attack	[21][24][31][35][37][39][42][60][65]
Ballot Stuffing Attack	[24][60]
On-off Attack	[28][31][33][35][40][65]
Conflicting Behavior Attack	[25][26][31][36][38][42][56][59][64][65]
Collusion Attack	[21][24][26][27][37][39][65]
Sinkhole Attack	[39][76]
Sybil Attack	[39][76]
DoS Attack	[36][37]

6. Future Research Directions

With the fast development and applications of wireless sensor networks especially in the field of Internet of Things, low computing complexity and high power efficiency become more and more important factors in securing the networks. When dealing with the internal attacks, reputation mechanism has received much attention by researchers, but still its related study is in the initial stage. Some future research directions regarding the binomial distribution based reputation are presented as follows.

1) How to properly set the reputation threshold. In most related literatures, the reputation threshold is a predefined value such as 0.5. One of the disadvantages is that in the network with frequent transactions, with the increasing number of node interactions, the reputation value of a good behaving node is increasing, but with the continuous depletion of the overall network energy, the number of transactions between nodes is declining, and so is the reputation value of the good behaving node. If a predefined reputation threshold is used, the reputation value of the good behaving node will eventually be lower than this threshold, and it may be misjudged as a malicious node, or even isolated by the network. Therefore, it is very necessary to design an adaptive reputation threshold that can meet the current network running state, and it can be adjusted adaptively under different conditions.

2) How to effectively set the forgetting factor. Like the reputation threshold, the forgetting factor is also set with a fixed value, which aims to give less weight to historical reputation parameters during the reputation fusion. However, in the network with low transaction frequency, the number of interactions between network nodes is not much. If this method is still used to set the forgetting factor, it is difficult to measure the current reputation state according to the past reputation parameters, and it is not conducive to the evaluation of nodes' reputation. Even malicious nodes can take advantage of it and launch attacks to further reduce the reputation of these nodes so as to destroy the normal operation of the network. Therefore, it is necessary to set the forgetting factor dynamically.

3) Few literatures have considered the redemption mechanism. The wireless sensor networks are usually deployed in unattended or even hostile areas where noise interference and environmental impact exist, which makes some good behaving nodes misjudged as malicious ones by the system. Therefore, in constructing the reputation system, it is necessary to consider the redemption mechanism so that nodes have the opportunity to work and serve the network again. In addition, penalty & reward mechanism should also be considered.

Reputation mechanism cannot motivate good behavior nodes at a faster speed, nor can it punish malicious nodes more quickly. Malicious nodes with high reputation still have the opportunity to attack the network. Thus, the penalty & reward mechanism can better help the network to make corresponding strategies for the good behaving nodes and malicious nodes.

4) Network attacks such as node replication attack and black hole attack cannot be addressed solely by the binomial reputation method. Binomial distribution based reputation is a light weight model and easy to be implemented in wireless sensor networks. But it has only two reputation parameters and its application scenarios are limited to a certain extent. Therefore, it is necessary to modify the binomial based reputation and design extra reputation parameters to better deal with more complex application scenarios.

Besides, some researchers suggest that methods such as machine learning and block chain be integrated into the reputation model. Although these methods can help further extend and improve the function of the reputation model, a trade-off should be made so that the energy can be balanced among each individual nodes and the network longevity can be improved.

7. Conclusion

As an effective supplement to the traditional security mechanism in wireless sensor networks, reputation has gradually attracted the attention of scholars. Among the reputation models, binomial distribution based reputation has many advantages such as light weight and ease of implementation in resource constraint sensor nodes. In this study, we perform a thorough survey and comment on existing binomial distribution based reputation models from the aspects of reputation engine, reputation fusion, and reputation aging. Based on the survey results, we believe that this study topic is still in the initial development and there are several open issues that should be solved. Thus we argue some open research problems and suggest the directions that are worth future efforts.

Acknowledgement

The authors gratefully acknowledge the helpful comments and suggestions of the reviewers.

References

[1] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni and Y. Yang, “Trust-based attack and defense in wireless sensor networks: a survey,” *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1-20, 2020. Article (CrossRef Link)

[2] W. Fang, N. Cui, W. Chen, W. Zhang and Y. Chen, “A Trust-Based Security System for Data Collection in Smart City,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4131-4140, 2021. Article (CrossRef Link)

[3] F. Azzedin and M. Ghaleb, “Internet-of-Things and information fusion: trust perspective survey,” *Sensors*, vol. 19, no. 8, pp. 1-22, 2019. Article (CrossRef Link)

[4] J. J. Jaramillo and R. Srikant, “A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks,” *Ad Hoc Networks*, vol. 8, no. 4, pp. 416-429, 2020. Article (CrossRef Link)

[5] S. Shen, G. Yue, Q. Cao and F. Yu, “A survey of game theory in wireless sensor networks security,” *Journal of Networks*, vol. 6, no. 3, pp. 521-532, 2011. Article (CrossRef Link)

[6] D. Lin and Q. Wang, “A game theory based energy efficient clustering routing protocol for WSNs,” *Wireless Netw*, vol. 23, pp. 1101–1111, 2017. Article (CrossRef Link)

[7] M. M. Mehdi, I. Raza and S. A. Hussain, “A game theory based trust model for vehicular ad hoc networks,” *Computer Networks*, vol. 121, pp. 152-172, 2017. Article (CrossRef Link)
[8] S. Liu, L. Zhang and Z. Yan, "Predict pairwise trust based on machine learning in online social networks: a survey," *IEEE Access*, vol. 6, pp. 51297-51318, 2018. Article (CrossRef Link)
[9] Y. Huang and M. Chen, "Improve reputation evaluation of crowdsourcing participants using multidimensional index and machine learning techniques," *IEEE Access*, vol. 7, pp. 118055-118067, 2019. Article (CrossRef Link)
[10] G. Han, Y. He, J. Jiang, N. Wang, M. Guizani and J. A. Ansere, "A synergetic trust model based on svm in underwater acoustic sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11239-11247, Nov. 2019. Article (CrossRef Link)
[11] J. Wang and et al., “A survey on trust evaluation based on machine learning,” *ACM Computing Surveys*, vol. 53, no. 5, pp. 1-37, 2020. Article (CrossRef Link)
[12] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and M. H. Rehmani, “Applications of blockchains in the internet of things: a comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2019. Article (CrossRef Link)
[13] A. Bellini, E. Bellini, M. Gherardelli, and F. Pirri, “Enhancing IoT data dependability through a blockchain mirror model,” *Future Internet*, vol. 11, no. 5, p. 117, May 2019. Article (CrossRef Link)
[14] M. Herlihy, “Blockchains from a distributed computing perspective,” *Commun. ACM*, vol. 62, no. 2, pp. 78–85, 2019. Article (CrossRef Link)
[15] E. Bellini, Y. Iraqi and E. Damiani, “Blockchain-based distributed trust and reputation management systems: a survey,” *IEEE Access*, vol. 8, pp. 21127-21151, 2020. Article (CrossRef Link)
[16] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University, Princeton, NJ, 1976.
[17] Y. Wu and et al., “A Dempster-Shafer theory based traffic information trust model in vehicular ad hoc networks,” in *Proc. of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, China, pp. 1-7, 2015. Article (CrossRef Link)
[18] A. Selvaraj and S. Sundararajan, “Evidence-based trust evaluation system for cloud services using fuzzy logic,” *Int. J. Fuzzy Syst.*, vol. 19, pp. 329–337, 2017. Article (CrossRef Link)
[19] C. Esposito, A. Castiglione and F. Palmieri, “Information theoretic-based detection and removal of slander and/or false-praise attacks for robust trust management with dempster-shafer combination of linguistic fuzzy terms,” *Concurrency and Computation: Practice and Experience*, vol. 30, no. 3, 2018. Article (CrossRef Link)
[20] A. Jøsang, “Trust and Reputation Systems,” *Lecture Notes in Computer Science in Foundations of Security Analysis and Design IV*, vol. 4677, pp. 209-245, 2007. Article (CrossRef Link)
[21] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” *ACM Transactions on Sensor Networks*, vol. 4, no. 3, pp. 1-37, 2008. Article (CrossRef Link)
[22] J. Lopez, R. Roman, I. Agudo and C. Fernandez-Gago, “Trust management systems for wireless sensor networks,” *Computer Communications*, vol. 33, no. 9, pp. 1086-1093, 2010. Article (CrossRef Link)
[23] F. G. Marmol and G. M.Perez, “Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems,” *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 185-196, 2010. Article (CrossRef Link)
[24] C. R. Perez-Toro, R. K. Panta and S. Bagchi, "RDAS: reputation-based Resilient data aggregation in sensor network," in *Proc. of 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Boston, MA, USA, pp. 1-9, 2010. Article (CrossRef Link)
[25] H. Feng and et al., “Trust based secure in-network data processing schema in wireless sensor networks,” *Journal of Networks*, vol. 6, no. 2, pp. 295-302, 2011. Article (CrossRef Link)

[26] H. Alzaid H., E. Foo and J. M. G. Nieto, “RSDA: Reputation-Based Secure Data Aggregation in Wireless Sensor Networks,” in *Proc. of 9th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2008*, Dunedin, Otago, New Zealand, pp. 419-424, 2008. Article (CrossRef Link)
[27] C. Liu, Y. Liu and Z. Zhang, “Improved reliable trust-based and energy-efficient data fusion for wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-11, 2013. Article (CrossRef Link)
[28] Z. Taghikhaki, N. Meratnia and P. J. M. Havinga, "Energy-efficient Trust-based aggregation in wireless sensor networks," in *Proc. of 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Shanghai, China, pp. 584-589, 2011. Article (CrossRef Link)
[29] M. Momani, S. Challa, *Probabilistic modelling and recursive bayesian estimation of trust in wireless sensor networks*, Bayesian Network, Chapter 23, 2010.
[30] B. Liu, Z. Xu, J. Chen and G. Yang, "Toward reliable data analysis for Internet of Things by Bayesian dynamic modeling and computation," in *Proc. of 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)*, Chengdu, China, pp. 1027-1031, 2015. Article (CrossRef Link)
[31] B. Liu and G. Yang, “Probabilistic trust evaluation with inaccurate reputation reports,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, pp. 1–7, 2015. Article (CrossRef Link)
[32] B. Liu and S. Cheng, “State space model based trust evaluation over wireless sensor networks: An iterative particle filter approach,” *Journal of Engineering*, vol. 2017, no. 4, pp. 101–109, 2017. Article (CrossRef Link)
[33] W. Fang and et al., “A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution,” *Sci. China Inf. Sci*. vol. 60, pp. 1-11, 2017. Article (CrossRef Link)
[34] Z. Liu, Z. Zhang, S. Liu, Y. Ke and J. Chen, "A Trust Model Based on Bayes Theorem in WSNs," in *Proc. of 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, China, pp. 1-4, 2011. Article (CrossRef Link)
[35] W. Fang, C. Zhu, W. Chen, W. Zhang and J. J. P. C. Rodrigues, "BDTMS: Binomial Distribution-based Trust Management Scheme for Healthcare-oriented Wireless Sensor Network," in *Proc. of 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 382-387, 2018. Article (CrossRef Link)
[36] X. Wu, J. Huang, J. Ling and L. Shu, "BLTM: beta and lqi based trust model for wireless sensor networks," *IEEE Access*, vol. 7, pp. 43679-43690, 2019. Article (CrossRef Link)
[37] W. Fang and et al, “BTRES: beta-based trust and reputation evaluation system for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 59, pp. 88-94, 2016. Article (CrossRef Link)
[38] Z. Zhou and N. Shao, “An improved trust evaluation model based on bayesian for wsns,” *Chinese Journal of Sensors and Actuators*, vol. 29, no. 6, pp. 927-933, 2016. Article (CrossRef Link)
[39] W. Fang and et al., "Binomial-based trust management system in wireless sensor networks,” *Chinese Journal of Sensors and Actuators*, vol. 28, no. 5, pp. 703-708, 2015. Article (CrossRef Link)
[40] W. Fang and et al., “Trusted scheme for defending on-off attack based on beta distribution,” *Journal of System Simulation*, vol. 27, no. 11, pp. 2722-2728, 2015. Article (CrossRef Link)
[41] A. Ahmed and A. R. Bhangwar, "WPTE: Weight-Based Probabilistic Trust Evaluation Scheme for WSN," in *Proc. of 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Prague, Czech Republic, pp. 108-113, 2017. Article (CrossRef Link)
[42] V. UmaRani, K. S. Sundaram and D. Jayashree, "Enhanced Beta Trust Model in wireless sensor networks," in *Proc. of 2016 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, pp. 1-5, 2016. Article (CrossRef Link)
[43] M. Zhang, "Trust computation model based on improved Bayesian for wireless sensor networks," in *Proc. of IEEE 17th International Conference on Communication Technology (ICCT)*, Chengdu, China, pp. 960-964, 2017. Article (CrossRef Link)

[44] C. Liu, Y. Liu, and Z. Zhang, "Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-11, 2013. Article (CrossRef Link)
[45] M. Mahmud and et al., "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," *Cogn Comput*, vol. 10, pp. 864–873, 2018. Article (CrossRef Link)
[46] L. Yang, J. M. Kizza, A. Cemerlic and F. Liu, "Fine-Grained Reputation-based Routing in Wireless Ad Hoc Networks," in *Proc. of IEEE International Conference on Intelligence and Security Informatics*, pp. 75-78, 2007. Article (CrossRef Link)
[47] Z. Yan, Y. Chen and Y. Shen, "A practical reputation system for pervasive social chatting," *Journal of Computer and System Sciences*, vol. 79, no. 5, pp. 556-572, 2013. Article (CrossRef Link)
[48] S. Buchegger, J. Mundinger and J. L. Boudec, "Reputation Systems for Self-Organized Networks," *IEEE Technology and Society Magazine*, vol. 27, no. 1, pp. 41-47, 2008. Article (CrossRef Link)
[49] Z. Bankovic and et al., "Detecting bad-mouthing attacks on reputation systems using self-organizing maps," *Computational Intelligence in Security for Information Systems, Lecture Notes in Computer Science*, vol. 6694, pp. 9-16, 2011. Article (CrossRef Link)
[50] Y. Yang and et al., "Defending online reputation systems against collaborative unfair raters through signal modeling and trust," in *Proc. of the ACM symposium on Applied Computing, Association for Computing Machinery*, New York, USA, pp. 1308–1315, 2009. Article (CrossRef Link)
[51] J. Hu and M. Burmeste, "LARS: a locally aware reputation system for mobile ad hoc networks," in *Proc. of the 44th annual Southeast regional conference, Association for Computing Machinery*, New York, USA, pp. 119–123, 2006. Article (CrossRef Link)
[52] F. Almenarez and et al., "Trust management for multimedia P2P applications in autonomic networking,"*Ad Hoc Networking*, vol. 9, no. 4, pp. 687-697, 2011. Article (CrossRef Link)
[53] R. Roman, M. Carmen and J. Lopez, "Featuring trust and reputation management systems for constrained hardware devices," in *Proc. of the 1st international conference on Autonomic computing and communication systems, Autonomics*, article no. 6, Rome, Italy, 2007. Article (CrossRef Link)
[54] F. G. Marmol and G. M. Perez, "Security threats scenarios in trust and reputation models for distributed systems," *Computer & Security*, vol. 28, no. 7, pp. 545-556, 2009. Article (CrossRef Link)
[55] M. Zhu, H. Chen and H. Wu, "A rank-based application-driven resilient reputation framework model for wireless sensor networks," in *Proc. of International Conference on Computer Application and System Modeling*, Taiyuan, China, pp. 125-129, 2010. Article (CrossRef Link)
[56] J. Li, R. Li and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 108-114, 2008. Article (CrossRef Link)
[57] Y. Yu and et al., "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867-880, 2012. Article (CrossRef Link)
[58] Y.Yu and et al., "Routing security scheme based on reputation evaluation in hierarchical ad hoc networks," *Computer Networks*, vol. 54, no. 9, pp. 1460-1469, 2010. Article (CrossRef Link)
[59] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Networks*, vol. 11, no. 4, pp. 1497-1509, 2013. Article (CrossRef Link)
[60] A. Jøsang and R. Ismail, "The beta reputation," in *Proc. of 15th Bled Electronic Commerce Conference e-Reality: Construction the e-Economy*, Bled, Slovenia, pp.324-327, 2002. Article (CrossRef Link)
[61] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," *Computer Communications*, vol. 31, no. 17, pp. 3941-3953, 2008. Article (CrossRef Link)

[62] P. Mukherjee and S. Sen, "Comparing Reputation Schemes for Detecting Malicious Nodes in Sensor Networks," *The Computer Journal*, vol. 54, no. 3, pp. 482-489, 2011. Article (CrossRef Link)
[63] Z. Bankovic and et al., "Bio-inspired enhancement of reputation systems for intelligent Environments," *Information Sciences*, vol. 222, pp. 99-112, 2013. Article (CrossRef Link)
[64] J. Feng and et al., "Reputation system for wireless sensor networks based on beta distribution," *Computer Applications*, 27, 111-113, 2007. Article (CrossRef Link)
[65] H. Chen, H. Wu, J. Hu and C. Gao, "Agent-Based Trust Management Model for Wireless Sensor Networks," in *Proc. of International Conference on Multimedia and Ubiquitous Engineering*, Busan, Korea (South), pp. 150-154, 2008. Article (CrossRef Link)
[66] N. Pissinou and G. V. Crosby, "Cluster-Based Reputation and Trust for Wireless Sensor Networks," in *Proc. of 4th IEEE Consumer Communications and Networking Conference*, Las Vegas, USA, pp. 604-608, 2007. Article (CrossRef Link)
[67] X. Xu, Y. Lin and S. Zhou, "Trust model based on beta distribution for sparse wireless sensor networks," *Application Research of Computers*, vol. 26, no. 6, pp. 2232-2234, 2009.
[68] S. Buchegger and J. L. Boudec, "A robust reputation system for P2P and mobile Ad-hoc Networks," in *Proc. of 2nd Workshop on the Economics of Peer-to-Peer Systems*, Cambridge, USA, pp. 1–6, 2004. Article (CrossRef Link)
[69] X. Liu, A. Datta and K. Rzadca, "Trust beyond reputation: A computational trust model based on stereotypes," *Electronic Commerce Research and Applications*, vol. 12, no. 1, pp. 24-39, 2013. Article (CrossRef Link)
[70] G. Casella, *Statistical Inference*, Duxbury Press, 1990.
[71] M. Momani, K. Aboura and S. Challa, "RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks," in *Proc. of 3rd International Conference on Intelligent Sensors, Sensor Networks and Information*, Melbourne, Australia, pp. 347-352, 2007. Article (CrossRef Link)
[72] D. V. Lindley and N. D. Singpurwalla, "Reliability and fault tree analysis using expert opinions," *Journal of the American Statistical Association*, vol. 81, no. 393, pp. 87-90, 1986. Article (CrossRef Link)
[73] M. West, "Bayesian aggregation," *Journal of Royal Statistical Society Series A*, vol. 147, no. 4, pp. 600-607, 1984. Article (CrossRef Link)
[74] S. Rackley, *Wireless Networking Technology: From Principles to Successful Implementation*, Newnes: 2007, ISBN-10: 0750667885.
[75] G. Yin and et al., "A novel reputation model for malicious node detection in wireless sensor networks," in *Proc. of 4th International Conference on Wireless Communications, Networking and Mobile Computing*, Dalian, China, pp.1-4, 2008. Article (CrossRef Link)
[76] Z. A. Khan, "Using energy-efficient trust management to protect IoT networks for smart cities," *Sustainable Cities and Society*, vol. 40, pp. 1-15, 2018. Article (CrossRef Link)

Zhe Wei received the Ph.D degree from Sichuan University, China, and he is currently an Associate Professor at Civil Aviation Flight University of China. His research interests include network security and IoT applications.

Shuyan Yu received the M.Sc degree from Beihang University, China in 2006, and she is currently a Professor at Shaoxing University Yuanpei College. Her research interests include deep learning and trusted computing.