Multi-Parameter and Time Series Based Trust for IoT Smart Sensors

Zhi-Ge He

(Corresponding author: Zhi-ge He)

School of Computer Science & Engineering, University of Electronic Science & Technology of China
No. 2006, Xiyuan Ave, West Hi-Tech Zone, 611731, Chengdu, Sichuan, P. R. China
(Email: 578301541@qq.com)

(Received Jan. 18, 2019; Revised and Accepted June 19, 2019; First Online July 16, 2019)

Abstract

The Internet of Things, or IoT has achieved much attention in the past few years with many concrete applications. Among various IoT components, smart sensors play a vital role for things' tracking and monitoring, but due to the absence of centralized administration, those sensors may encounter various security issues which hinder IoT further development. Trust computing provides dynamic behavior perceiving capability and can take precautionary measures against malicious actions. In this study, unlike traditional binary parameter trust, we first propose a multi-parameter trust computing method so that trust states can be more accurately and practically described, then according to the theory of time series, a favorable trust data sequence and an unknown trust data sequence are generated so that nodes' malicious actions can be observed and detected from the context of a time period. Simulation results show that the proposed method can generate a fast detection of malicious nodes, a higher data packet delivery ratio, and a more trusted network environment ideal for transactions among sensor nodes.

Keywords: IoT; Multi-Parameter Trust; Smart Sensors; Time Series

1 Introduction

As one of the most emerging technologies in computer science, the Internet of Things, or IoT has achieved much popularity in the past few years and many IoT applications are being implemented in areas like logistics, traffic surveillance, and smart families. IoT can incorporate seamlessly and transparently a large number of heterogeneous smart devices or end systems, while providing open access to selected subsets of data for the development of a great many of digital services [21,24]. The term IoT is initially used to refer to the interoperability of uniquely identifiable objects with radio frequency identification (RFID) technology [16]. Later, the definition of IoT has been expanded to refer to a network of interconnected objects or devices such as RFID tags, sensors, actuators, and smart phones with the object to collect data and interact with the physical world [3, 22].

Among various IoT components, smart sensors play a vital role in the current IoT applications. Programmable smart sensors equipped with processing unit, storage memory, and wireless communication module are able to autonomously join in or construct a certain IoT network. Those sensors usually work in a completely distributed manner so as to collaboratively collect ambient data and monitor certain events. But due to the lack of fixed infrastructure, the absence of centralized administration, and the inherent characteristics of these sensors such as limited computing resources, short radio range, and dynamic topology, IoT composed by those sensors may encounter various security issues, *e.g.*, an entity may become malicious and launch packet dropping or select forwarding attack to gain its own benefits, which poses new security challenges for IoT applications [10, 15, 20].

As a complementary solution to the traditional network security, trust mechanism provides access control by judging the quality of the service and makes traditional security services more reliable by ensuring that all communicating devices are trustworthy during service cooperation [13, 14]. In this study, unlike traditional binary parameter trust methods [8], we first propose a multi-parameter trust computing method so that trust states can be more accurately and practically described, then according to the theory of time series, a favorable trust data sequence and an unknown trust data sequence are generated so that nodes' malicious actions can be observed and detected from the context of a time period.

The rest of this study is organized as follows. Section 2 explores recent representative trust-based models implemented for the IoT. Section 3 describes the preliminaries about trust computing and theory of time series. Sections 4 and 5 present our proposed trust method and related simulation tests. Section 6 concludes this article and suggests directions for future research.

2 Related Work

In this section, some latest and representative literatures about trust schemes in IoT are discussed, ranging from data aggregation/fusion, edge computing, malicious infiltration, information sharing, data routing, node classification, to trust estimation and assessment.

Data aggregating techniques using external IoT mobile elements (MEs) have been recently proposed in some studies where MEs collect data from stationary sensors and relay the collected data to the base station. These MEs could be regular mobile sensors or any mobile devices with sensing capability. Ali *et al.* [3] proposed a scheme on selecting trusted MEs for data aggregation in IoT enabled wireless sensor networks. When passing through the network, only trusted MEs were recruited, then they acted as anonymous agents and served as the cluster heads in order to increase the life span of the network. The trust vales placed on MEs were completely based on the direct interactions between the MEs and the base station at the end of each aggregation round. Regarding the trust calculation, [3] also uses the classic Beta trust model [8] which is of two trust parameter based and has been utilized by many reputation systems for its simplicity and flexibility. After that, all the trust values and management are handled by the base station and each sensor node maintains a local copy of the trust vales for other nodes in the network.

The integration of IoT and edge computing is currently a hot research direction, but the lack of trust among IoT edge devices has somewhat hindered the acceptance of IoT edge computing [19]. To facilitate the IoT edge computing applications, Yuan *et al.* [23] proposed a reliable and lightweight trust mechanism for IoT edge devices based on multi-source feedback information fusion so that efficient trust calculation mechanism can be established in the IoT edge computing architecture. The proposed scheme uses a feedback information fusion algorithm based on objective information entropy theory to overcome the limitations of traditional trust schemes, and the trust factors can be weighted manually or subjectively. In [23], the trust calculation falls into direct trust calculation and feedback trust calculation. The former uses the similar Beta trust model and the latter maintains the trust vales in a matrix.

Infiltration from malicious devices that can temporarily stop the provided services is one of the main issues faced by the current IoT networks and these malicious devices may also launch coordinated attacks. To find out the malicious behavior of IoT nodes, Khan [12] proposed an intrusion detection system based on the trust management where a node monitored the receivers of its messages checking if they had forwarded them correctly. Behavior following the scheme can improve the trust of a node in another one, but trust deteriorates if the observer detects that its peer behaves maliciously. [12] built the trust relation by using the opinion triangles in Jøsang's subjective logic [11] which allows to aggregate the trust values of various other IoT devices.

For information sharing in a health IoT system comprising IoT devices carried by members of an environmental health community, Al-Hamadi *et al.* [2] proposed a trust management system that could guide IoT devices to use the most trustworthy environmental health information for decision making. In [2], a collective knowledge base can be built to rate the environment at a particular location and time, and this knowledge could enable an IoT device to act on behalf of its user to decide whether or not the user should visit this place for health reasons. The proposed system considers the risk classification, reliability trust, and loss of health probability for decision making in the health IoT system.

With large amount of IoT devices likely to be interconnected globally, an important issue is how to secure the routing of data in the underlying networks from various attacks. Airehrour *et al.* [1] proposed a lightweight secure trust-based routing framework for IoT sensor nodes to identify and isolate common routing attacks in IoTs. The proposed framework incorporates the concept of trust among different IoT sensor nodes and utilizes the successful and unsuccessful node interactions among IoT nodes to evaluate a neighbor's trustworthiness. Further, the framework also considers a recovery period for nodes that are classified as untrusted ones owing to lossy network links or low battery power which could result in the decrease of their trust values.

Fragkiadakis *et al.* [7] proposed a centralized trust-based scheme employing evidence reasoning for IoT architecture where all nodes monitor their one-hop neighbors and report their findings to a single fusion center. The proposed scheme considers nodes' behavior with regards to their forwarding capability, thus each node observes its neighbors and estimates their packet drop ratio, then all nodes create direct trust reports for specific criteria regarding their neighbors, and the fusion is performed by employing a belief distribution using an evidence reasoning algorithm.

Asiri *et al.* [4] proposed an IoT trust and reputation model which used distributed probabilistic neural networks to classify trustworthy nodes from malicious ones. The proposed model is based on a recommender system which helps an IoT node decide to connect to another one based on previous observed behaviors. The proposed model also tackles the cold start problem in IoT environment by predicting ratings for newly joined nodes based on their characteristics over time, and the processing is completely distributed and is handled by the nodes themselves.

Gwak *et al.* [9] proposed an IoT trust estimation scheme making a user evaluate the trust value of an IoT device in an unknown place. The proposed scheme is on the basis that a user's subjective experience can be substituted by those social friends sharing identical subjective experiences with the user. It first finds a collection of past subjective experiences of a user relevant to the target device, then it discovers the friends of a target user who

have past subjective experiences closely matching with the collection. Based on the subjective trust value and the level of the subjective experience identity of the sharing friends, a user's trust value of a target device with the objective opinion of all the users who have interacted with the device is estimated.

To establish the initial trust level that a device places on another at their first encounter in IoTs, Nguyen *et al.* [17] proposed a challenge-response-based initial trust assessment scheme. The proposed scheme creates the knowledge about the device by learning the uncertainty level in its behaviors, then it relies on the results of the challenge-response process to assess if a device can be trusted to a level for its admission to the network. The proposed mechanism allows a device to generate the evidence for trust computation instead of waiting for the recommendations or actual interactions for long period.

3 Preliminaries

In this section, as the basis of our proposed trust method, we first discuss the traditional trust computing method and then shortly introduce the theory of time series.

3.1 Trust Computing

In trust computing, Bayesian analysis [5] has been widely used, and as a representative of such a approach, Ganeriwal *et al.* [8] proposed a classical reputation based framework for high integrity sensor networks (RFSN) where sensor nodes use Beta reputation to evaluate other's trust values.

Suppose that in a packet relay cooperation, a sensor node i has the probability φ to pass a packet to another node in the following jth round, let α and β denote the historical number of successful and unsuccessful cooperations respectively, φ is an unknown parameter and is equally to take all the values between 0 and 1 inclusive, then according to Bayesian analysis, $P(\varphi)$ is defined by

$$P(\varphi) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\varphi^{\alpha-1}(1-\varphi)^{\beta-1} \tag{1}$$

Let $K(=0/1)$ denote the outcome of the jth round, then $P(K|\varphi)$ is defined by

$$P(K|\varphi) = \varphi^K(1-\varphi)^{1-K} \tag{2}$$

Once the jth round is completed, according to Bayesian theorem, the posterior distribution of φ is defined by

$$P(\varphi|K) = \frac{P(K|\varphi)P(\varphi)}{\int P(K|\varphi)P(\varphi)d\varphi} \tag{3}$$

Put Equation 1 and Equation 2 into Equation 3, then we get

$$\begin{aligned} P(\varphi|K) &= \frac{\varphi^K(1-\varphi)^K\frac{\Gamma(\alpha+\beta)\cdot\varphi^{\alpha-1}(1-\varphi)^{\beta-1}}{\Gamma(\alpha)\Gamma(\beta)}}{\int \varphi^K(1-\varphi)^{1-K}\cdot\frac{\Gamma(\alpha+\beta)\cdot\varphi^{\alpha-1}(1-\varphi)^{\beta-1}}{\Gamma(\alpha)\Gamma(\beta)}d\varphi} \\ &= \frac{\Gamma(\alpha+\beta+1)\varphi^{\alpha+K-1}(1-\varphi)^{\beta+1-K-1}}{\Gamma(\alpha+K)\Gamma(\beta+1-K)} \end{aligned} \tag{4}$$

Equation 4 is the update of φ after the jth round. It can be noticed that in Equation 4, the posterior probability of φ still has a Beta distribution, i.e. before the jth round, $P(\varphi) \backsim Beta(\alpha,\beta)$ (Equation 1) ; after the jth round, $P(\varphi) \backsim Beta(\alpha+K, \beta+1-K)$. Therefore, before the jth round, $E(\varphi)$ is defined by

$$E(\varphi) = \frac{\alpha}{\alpha+\beta} \tag{5}$$

and after the jth round, $E(\varphi)$ is redefined by

$$E(\varphi) = \frac{\alpha+K}{\alpha+\beta+1} \tag{6}$$

In practice, $E(\varphi)$ is the trust value of node i and (α,β) are the only two trust parameters characteristic of Beta reputation that are computed and maintained by the neighboring nodes. This kind of trust computing is also called direct observation computing, and many literatures like [3,17] either directly or indirectly extend and modify such a method. In [18], an indirect method based on the belief discounting is used in the trust system, which is mapped into Dempster-Shafer belief theory [6] where the two trust parameters are defined as follows.

$$\alpha_i+ = \frac{2\alpha_h\alpha_i^h}{(\beta_h+2)+(\alpha_i^h+\beta_i^h+2)+2\alpha_h} \tag{7}$$

$$\beta_i+ = \frac{2\alpha_h\beta_i^h}{(\beta_h+2)+(\alpha_i^h+\beta_i^h+2)+2\alpha_h} \tag{8}$$

In Equation 7 and Equation 8, j receives the trust about i from h, let (α_i^h,β_i^h) denote the indirect trust and j has the past trust values about i and h denoted by (α_i,β_i) and (α_h,β_h) respectively. One of the advantages of the indirect method is that malicious nodes are prevented from colluding with each other to feed false trust information, but it can also result in the energy exhaustion of the network system.

To sum up, Beta reputation first computes the prior probability of an event, then updates the probability by using a posterior inference according to the relevant evidences, and (α,β) are trust parameters used to represent the positive and negative outcome in a transaction. Although Beta reputation model is widely used, it only considers two parameters to describe an event, which limits its applications to a large extent.

3.2 Time Series

Time series is a statistics tool for processing dynamic data sequence by which meaningful or abnormal facts can be analyzed and discovered. The data sequence is usually measured at successive time instants and spaced at predefined time intervals. For example, let Y denote a random variable and its time series is defined by $Y=\{y_1,...,y_n\}$ where y_n is the value of Y at time instant n.

In an IoT network, a node's trust is directly related to its *attitude* towards certain task, *e.g.*, faithfully relay data

packets as requested, or maliciously drop some or all the data packets. To some extent, malicious actions always end up with lower trust, but smart sensors can switch between *good* and *bad* so as to keep their trust and cover their malicious actions. Such a switch is easy to result in trust fluctuation over time. Thus, the fluctuated trust values can be regarded as a data sequence, and time series can be used to find out whether a node is of malicious actions or not.

In a trust data time series, there are three components: a trust data sequence to be checked, a standard sequence to be compared with, and a sequence checking mechanism. The trust data sequence is the outcomes of a certain node actions over time, *e.g.*, node i's trust data sequence is defined by

$$\mathcal{T}_i = \{t_i(t_1), t_i(t_2), ..., t_i(t_n)\}. \tag{9}$$

The standard sequence consists of a series of comparing data, each of which will be compared with its counterpart of the same time instant in the trust sequence. The standard sequence is denoted by

$$\mathcal{S} = \{s(t_1), s(t_2), ..., s(t_n)\}. \tag{10}$$

Both the trust data sequence and the standard sequence should have the same length, and the sequence checking mechanism used in this article will be introduced in the following section.

4 The Proposed Method

In this section, our proposed multi-parameter and time series base trust method is presented. The proposed method consists of two components: a trust computing module and a time series checking module.

4.1 Trust Computing Module

Assume there are k outcomes in one transaction denoted by $\{o_1, ..., o_k\}$ with the probability $\Theta = \{\theta_1, ..., \theta_k\}$ where $P(o_i) = \theta_i$, and n_i is the number of occurrence of o_i where $n_1 + n_2 + ... + n_k = N$, then according to the multinomial distribution, $P(Y = N|\Theta)$ is defined by

$$P(Y = N|\Theta) = \Sigma_{i=1}^{k-1} n_i \cdot (N-1)! \cdot \frac{\Pi_{i=1}^{k} \theta_i^{n_i}}{\Pi_{i=1}^{k} n_i!} \tag{11}$$

Based on the Dirichlet distribution, the conjugate prior probability of Θ is defined by

$$P(\Theta) = \frac{\Gamma(\Sigma_{i=1}^{k} \alpha_i)}{\Pi_{i=1}^{k} \Gamma(\alpha_i)} \cdot \Pi_{i=1}^{k} \theta_i^{\alpha_i - 1} \tag{12}$$

In Equation 12 as in Equation 1, α_i is the prior or historical counts of o_i, and the posterior of Θ is defined by

$$P(\Theta|Y = N) = \frac{P(Y = N|\Theta)P(\Theta)}{\int P(Y = N|\Theta) d\Theta} \tag{13}$$

Put Equation 11 and Equation 12 into Equation 13, we get

$$P(\Theta|Y = N) = \frac{\Sigma_{i=1}^{k-1} n_i \cdot (N-1)! \cdot \frac{\Pi_{i=1}^{k} \theta_i^{n_i}}{\Pi_{i=1}^{k} n_i!} P(\Theta)}{\int \Sigma_{i=1}^{k-1} n_i \cdot (N-1)! \cdot \frac{\Pi_{i=1}^{k} \theta_i^{n_i}}{\Pi_{i=1}^{k} n_i!} d\Theta} \tag{14}$$

$$= \frac{\Sigma_{i=1}^{k-1} n_i \cdot (N-1)! \cdot \frac{\Pi_{i=1}^{k} \theta_i^{n_i}}{\Pi_{i=1}^{k} n_i!} \cdot \frac{\Gamma(\Sigma_{i=1}^{k} \alpha_i)}{\Pi_{i=1}^{k} \Gamma(\alpha_i)} \cdot \Pi_{i=1}^{k} \theta_i^{\alpha_i - 1}}{\int \Sigma_{i=1}^{k-1} n_i \cdot (N-1)! \cdot \frac{\Pi_{i=1}^{k} \theta_i^{n_i}}{\Pi_{i=1}^{k} n_i!} d\Theta}$$

$$= \frac{\Gamma(\Sigma_{i=1}^{k} (\alpha_i + n_i))}{\Pi_{i=1}^{k} \Gamma(\alpha_i + n_i)}$$

Then, $E(\Theta)$ is defined by

$$E(\Theta) = (\frac{\alpha_1 + n_1}{\sum_{i=1}^{k} (\alpha_i + n_i)}, ..., \frac{\alpha_k + n_k}{\sum_{i=1}^{k} (\alpha_i + n_i)}). \tag{15}$$

In Equation 15 as in Equation 6, $E(\Theta)$ is the trust value set of node i and $(\alpha_1, ..., \alpha_n)$ are the multi trust parameters characteristic of the trust computing model in the proposed method where in $\alpha_i + n_i$, $n_i = 0, 1, ...N$.

Consider an example of three kinds of outcomes, assume that they are {*excellent, good, average*} denoted respectively by $\{o_1, o_2, o_3\}$ with the occurrence number $\{n_1, n_2, n_3\}$ after certain transactions, and the historical occurrence numbers are $\{\alpha_1, \alpha_2, \alpha_3\}$, based on Equation 15, the trust value set of {*excellent, good, average*} are computed as follows.

$$E(\theta_1) = \frac{\alpha_1 + n_1}{\alpha_1 + \alpha_2 + \alpha_3 + n_1 + n_2 + n_3} \tag{16}$$

$$E(\theta_2) = \frac{\alpha_2 + n_2}{\alpha_1 + \alpha_2 + \alpha_3 + n_1 + n_2 + n_3} \tag{17}$$

$$E(\theta_3) = \frac{\alpha_3 + n_3}{\alpha_1 + \alpha_2 + \alpha_3 + n_1 + n_2 + n_3} \tag{18}$$

Compared with the Beta reputation based trust, the multi parameter based trust has more trust parameters to present more outcome states in the actual applications.

4.2 Sequence Checking Module

In the checking module, the trust data sequence and the standard sequence are regarded as two vectors, the cosine angle $\lambda(v_1, v_2)$ of the two vectors are computed to measure their similarity, regarding the trust data sequence and the standard sequence, their cosine angle is defined by

$$\lambda(\mathcal{T}_i, \mathcal{S}) = \frac{\mathcal{T}_i \cdot \mathcal{S}}{\| \mathcal{T}_i \| \| \mathcal{S} \|} = \frac{\sum_{j=1}^{n} t_i(t_j) \times s(t_j)}{\sqrt{\sum_{j=1}^{n} (t_i(t_j))^2} \times \sqrt{\sum_{j=1}^{n} (s(t_j))^2}} \tag{19}$$

Further, λ is formalized as follows so that its value is mapped into $[0, 1]$.

$$\dot{\lambda}(\mathcal{T}_i, \mathcal{S}) = 1 - \frac{\cos^{-1}(\lambda(\mathcal{T}_i, \mathcal{S}))}{\pi} \tag{20}$$

In Equation 20, the closer $\dot{\lambda}$ gets to 0, the less similar the trust data sequence and the standard sequence become, which means that the trust data sequence deviates from the standard sequence to a large extent, and the sensor node is highly likely of malicious actions within the time period.

In practice, considering the unknown events such as packet loss during the transmission and to fully take the advantage of the multi trust parameters, we use four data sequences: favorable trust data sequence fT_i (like successful data relay) and its counterpart comparing standard sequence S_{fT}, unknown trust data sequence uT_i and its comparing standard sequence S_{uT}.

The working algorithm of the proposed trust method is shown in Algorithm 1.

Algorithm 1 Working of the proposed method

α_1: historical favorable outcome number
α_2: historical unfavorable outcome number
α_3: historical unknown outcome number
n_1: current favorable outcome number
n_2: current unfavorable outcome number
n_3: current unknown outcome number
Len: segment length of time series measured by the number of transactions ($Len \geq n_1 + n_2 + n_3$)
$\varphi_1 \in [0, 1]$: threshold of $\dot{\lambda}(fT_i, S_{fT})$
$\varphi_2 \in [0, 1]$: threshold of $\dot{\lambda}(uT_i, S_{uT})$
Begin
Node j initiates a certain transaction such as packets relay within its one hop neighbors, assume Node i responds, j first checks i's (favorable) trust value, if i is qualified then j starts the transaction with i and observes i's transaction outcomes
for(count=0, count <= *Len*, count++)
  {j observes the transaction outcomes and records them in (n_1,n_2,n_3)}
if ($\dot{\lambda}(fT_i, S_{fT}) > \varphi_1$)
  {$\alpha_1 += n_1, \alpha_2 += n_2, \alpha_3 += n_3$, compute $E(\theta_1)$}
else
{
  if ($\dot{\lambda}(uT_i, S_{uT}) > \varphi_2$)// i is of malicious actions.
    {delete i from j's transaction partners' list, or reset i's trust value for its redemption}
  else// too many unknown outcomes exist.
    {$\alpha_1 = \alpha_1, \alpha_2 = \alpha_2, \alpha_3 += n_3$, compute $E(\theta_1)$}
}
End

5 Simulations

Suppose that in an IoT packet relay task, there exist three kinds of smart sensor nodes, i.e. legitimate nodes (65%), malicious nodes (25%), and selfish nodes (10%). A transaction is defined as a data packet relay. Legitimate nodes are of good actions and they faithfully relay all the received packets to the others as requested; to attack the integrity of network is the first priority of the malicious nodes, they intelligently and selectively drop some or all the received packets and try to keep their trust values to an acceptable level so as to cover their malicious actions; selfish nodes sometimes drop packets or deny request not out of malicious actions but to gain its own benefit such as saving their energy. Each node generates 1 data packet containing its ID on every 10 seconds, and a base station locates on the border of the test area to collect all the packets from the network. It is also assumed that sensor nodes are capable of bidirectional communication and their NICs work in a promiscuous mode. NS–2 is used for simulation and the classical binary reputation based trust used in [3] is selected for comparing. Simulation parameters are presented in Table 1.

Table 1: Simulation parameters

Parameters	Values
Simulation time	500s
Number of nodes	100
Test area	$200\times200m^2$
Transmission range	50m
Node placement	random
MAC protocol	IEEE 802.11
Packet size	100 bytes
Communication error	5%
S_{fT}	randomly $\subset [0.75, 0.95]$
uT_i	randomly $\subset [0, 0.15]$
Initial trust value	0.5

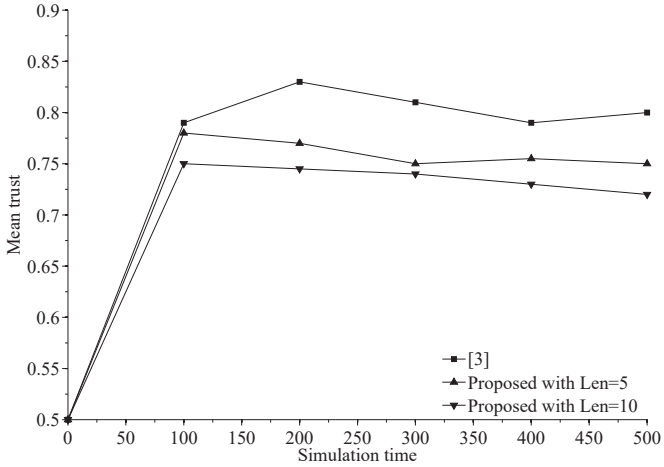

Figure 1: Mean trust with $\varphi_1 = 0.8, \varphi_2 = 0.8$

5.1 Test 1

In this section, the mean trust value is tested between the compared method and the proposed method, results are shown in Figure 1 and Figure 2.

In Figure 1, as the simulation time goes by, the mean

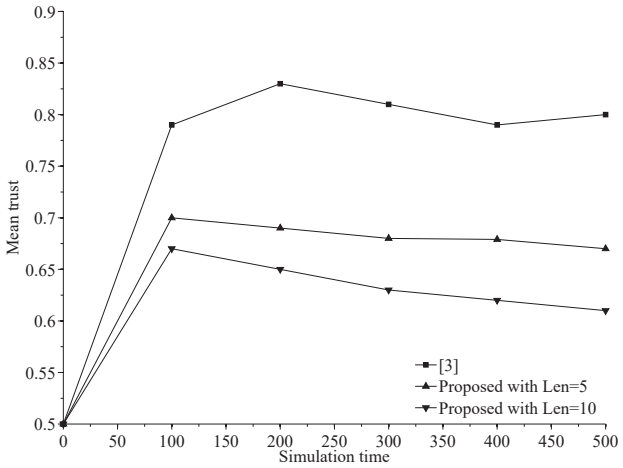

Figure 2: Mean trust with $\varphi_1 = 0.9, \varphi_2 = 0.9$

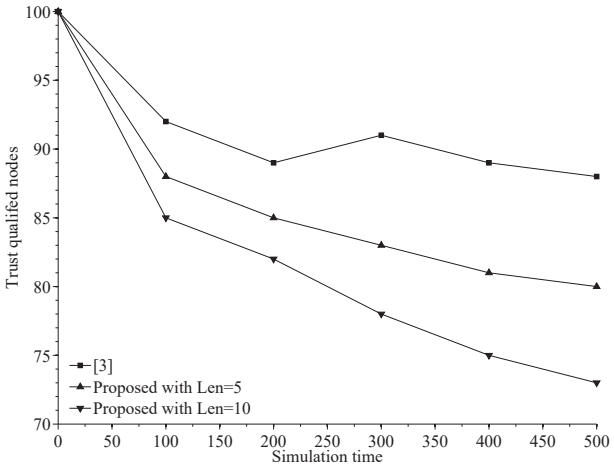

Figure 3: Trust qualified nodes with $\varphi_1 = 0.8, \varphi_2 = 0.8$

trust value in [3] begins to go upward and reaches about 0.83 on the 200th second, then drops and fluctuates around 0.8 till to the 500th second. Although there exist 25% malicious nodes and 10% selfish nodes, the mean trust value still keeps high as 0.8. This is because in [3], malicious nodes can intelligently switch between passing and dropping the packets, which helps them maintain an acceptable trust value that can be considered as trusted relaying nodes.

While in the proposed method, trust is computed based on *Len*–segment length of time series which is measured by the number of transactions. It means that trust in the proposed method is computed according to the segment length instead of upon the completion of a transaction. This helps to keep broader perspective on the target nodes. When malicious nodes intelligently switch between *good* and *bad*, its trust fluctuate accordingly, when its trust data sequence and standard data sequence are applied into the checking module, if the result is less than the threshold φ_1 and meanwhile there is no enough unknown outcomes, then according to the algorithm presented above, such nodes are treated as malicious ones. In Figure 1, it can be noticed that due to the successfully spotting the malicious nodes, the mean trust value in the proposed method goes downward gradually, *e.g.*, around 0.67 ($Len = 5$) and 0.63($Len = 10$) on the 500th second. In Figure 1, the mean trust is the lowest in the propose method when the $Len = 10$, this is because when *Len* becomes larger, more malicious actions can be observed, if any, and malicious nodes are more difficult to cover their actions.

Similar results can be found in Figure 2. The difference is that in Figure 2, the thresholds φ_1 and φ_2 are set as 0.9 instead of 0.8 in Figure 1. Figure 2 shows that when these two thresholds are set larger, the checking module is becoming stricter, meaning that more malicious nodes can be detected resulting in much lower mean trust of the the network, *e.g.*, around 0.6 when ($Len = 5$) on the 500th second in Figure 2.

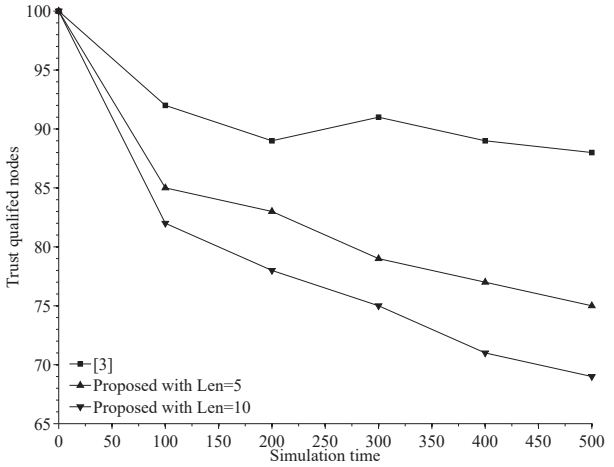

Figure 4: Trust qualified nodes with $\varphi_1 = 0.9, \varphi_2 = 0.9$

5.2 Test 2

In this section, the number of trust qualified nodes is tested between the compared method and the proposed method, results are shown in Figure 3 and Figure 4.

As is shown in Figure 3 and Figure 4, as the simulation continues, the number of trust qualified nodes drops in both the compared methods, *e.g.*, in Figure 3, the number in [3] is around 90 on the 200th second and around 88 on the 500th second. Such a number varies slightly from the 200th second to the 500th second, and the reason is that the switching actions of malicious nodes make them difficult to be spotted by the method in [3]. In addition, the number of trust qualified nodes of [3] in Figure 3 or Figure 4 is not the actual number which consists of many malicious nodes.

On contrast, the number of trust qualified nodes drops

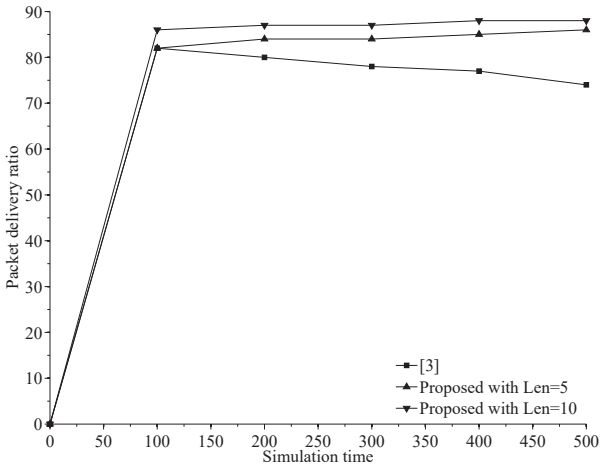

Figure 5: Packet delivery ratio with $\varphi_1 = 0.8, \varphi_2 = 0.8$

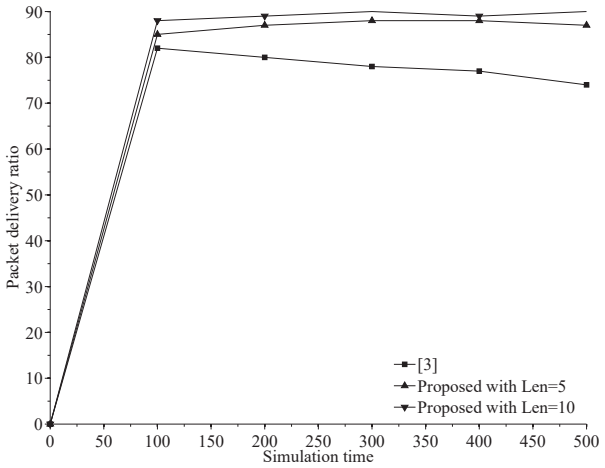

Figure 6: Packet delivery ratio with $\varphi_1 = 0.9, \varphi_2 = 0.9$

faster in the proposed method, *e.g.*, in Figure 3, around 86 on the 200th second and around 81 on the 500th second when $Len = 5$. In Figure 3 and Figure 4, it can be found that both the segment length Len and the two thresholds φ_1, φ_2 influence the number of trust qualified nodes. Under the same conditions, the larger the segment length and the two thresholds get, the less number of the trust qualified nodes becomes. For example, in Figure 4, when $Len = 10$, $\varphi_1 = 0.9$, and $\varphi_2 = 0.9$, the number in the proposed method is around 69. However, such a number in the proposed method approximates the actual number of legitimate nodes (65%), meaning that more and more malicious nodes including some selfish nodes are detected in the proposed method and most of the remaining nodes are legitimate.

5.3 Test 3

In this section, the packet delivery ratio is tested between the compared methods and results are shown in Figure 5 and Figure 6.

Due to the existence of malicious nodes and selfish nodes, not all the data packets generated by the legitimate nodes can be received by the base station. Take Figure 6 as an example, on the 500th seconds, only about 75% data packets reach the base station, and most of the rest 25% are dropped by the malicious nodes; while in the proposed method, because of the timely detection of malicious nodes, the packet delivery ration can reach as high as 85% ($Len = 5$) or 90% ($Len = 10$). Figure 5 and Figure 6 further indicate that with the increase of segment length and the two thresholds φ_1, φ_2, so does the packet delivery ratio.

These three tests also indicate that compared with the method in [3], although the proposed method generates a lower mean trust value and less trust qualified nodes in the network, it does result in a fast detection of malicious nodes, a higher data packet delivery ratio, and a more trusted network environment ideal for transactions among sensor nodes.

6 Conclusions

Due to the lightweight but powerful mechanism, trust scheme is a promising technology to establish security for the resource-constrained devices that are characteristic of the IoT smart sensors. In this study, we propose a multi-parameter trust computing method combined with the theory of time series. Through simulation tests, the feasibility and effectiveness of the proposed method have been confirmed. But in the proposed method, the segment length, the two thresholds cannot be selected freely, a longer segment length would exhaust the buffer of a sensor node; a larger threshold would not tolerate any mistakes such as a single packet dropping in the test case; a smaller threshold would be availed by malicious nodes to switch their actions, all of which would be our future research.

Acknowledgments

This study was supported by the NSF of China under grant No. 61772115 and Sichuan Miaozi Project under grant No.2019009. The author gratefully acknowledges the anonymous reviewers for their valuable comments.

References

[1] D. Airehrour and *et al.*, "A lightweight trust design for IoT routing," in *The 14th IEEE International Conference on Pervasive Intelligent and Computing*, pp. 552-557, 2016.

[2] H. Al-Hamadi and I. R. Chen, "Trust-based decision making for health IoT systems," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1408-1419, 2017.

[3] B. A. Ali, H. M. Abdulsalam and A. Alghemlas, "Trust based scheme for IoT enabled wireless sensor networks," *Wireless Personal Communications*, vol. 99, no. 4, pp. 1061-1080, 2018.

[4] S. Asiri and A. Miri, "An IoT trust and reputation model based on recommender systems," in *Privacy, Security & Trust*, pp. 561-568, 2017.

[5] S. Che and *et al.*, "A lightweight trust management based on Bayesian and entropy for wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 168-175, 2015.

[6] A. Dempster, "Upper and lower probabilities induced by multivalued mapping," *The Annals of Mathematical Statistics*, vol. 38, no. 2, pp. 325-339, 1967.

[7] A. Fragkiadakis and E. Tragos, "A trust-based scheme employing evidence reasoning for IoT architectures," in *IEEE World Forum on Internet of Things*, pp. 559-564, 2017.

[8] S. Ganeriwal and *et al.*, "Reputation based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, pp. 15-37, 2008.

[9] B. Gwak and *et al.*, "IoT trust estimation in an unknown place using the opinions of i-sharing friends," in *IEEE Trustcom*, pp. 602-609, 2017.

[10] R. Jhaveri and *et al.*, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile Ad-Hoc networks in industrial IoT," *IEEE Access*, vol. 6, pp. 20085-20103, 2018.

[11] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, pp. 279-311, 2001.

[12] 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.

[13] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[14] X. Li and *et al.*, "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1402-1415, 2015.

[15] L. Liu, Z. Cao, O. Markowitch, "A note on design flaws in one aggregated-proof based hierarchical authentication scheme for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 88–92, 2016.

[16] A. Mayzaud, R. Badonnel and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459-473, 2016.

[17] T. Nguyen and *et al.*, "Initial trust establishment for personal space IoT systems," in *IEEE Conference on Computer Communications Workshops*, pp. 784-789, 2017.

[18] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," *Computer Communications*, vol. 31, no. 17, pp. 3941-3953, 2008.

[19] S. Pinto and *et al.*, "IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices," *IEEE Internet Computing*, vol. 21, no. 1, pp. 40-47, 2017.

[20] J. Shen and *et al.*, "Cloud aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 105, pp. 117-123, 2018.

[21] R. Singh and M. S. Manu, "An energy efficient grid based static node deployment strategy for wireless sensor networks," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 32-40, 2017.

[22] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[23] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626-23638, 2018.

[24] A. Zanella and *et al.*, "Internet of things for smart cities," *Internet of things for smart cities*, vol. 1, no. 1, pp. 22-32, 2014.

Biography

Zhi-ge He. He received his bachelor degree in computer science and application from University of Electronic Science and Technology of China in 2017 and now he is a master candidate in computer science and application. His main research interest includes network security and big data.