ISSN 2278-5612

Cognitive Internet of Things-Oriented Multi-Domain Cooperation Dynamic Incentive Mechanism based on Reputation

Tenghao Li, Ruijuan Zheng, Ying Li, Qingtao Wu, Mingchuan Zhang, Wangyang Wei, Zhengchao Ma

Electronic & Information Engineering College, Henan University of Science and Technology, Luoyang 471003, China

litenghao923@163.com

rjwo@163.com

lying_511@163.com

ABSTRACT

As a new ubiquitous network, Internet of Things (IoT, for short) is widely used in various fields, which has a huge network, diverse sensor nodes, multifarious communication protocol. The resource management in IoT is difficult and the application fields are also expanding. Meanwhile, complexity, uncertainty and ambiguity of IoT also contribute toward the development direction of "comprehensive cognition", "intelligent decision", so the introduction of cognitive elements into the IoT to constitute Cognitive Internet of Things (CIoT, for short) is particularly important. In allusion to the possible negative packets forward problem of selfish nodes in CIoT, we proposed a multi-domain cooperation dynamic incentive mechanism based on reputation in CIoT (C2R, for short). According to the characteristics of CIoT and the QoS requirements of the users, dynamic reputation evaluation between nodes is used to achieve the self-management of the network and motivate selfish nodes to forward packets. Meanwhile, multi-domain cooperative idea expands the application scope. The simulation results show that the mechanism can better enhance the network availability, and has a good performance in packets loss and throughput.

Indexing terms/Keywords

Cognitive Internet of Things; Multi-Domain Cooperation; Reputation Evaluation; Dynamic Incentive Mechanism.

Academic Discipline And Sub-Disciplines

Application research of networks

SUBJECT CLASSIFICATION

Autonomous management of networks

TYPE (METHOD/APPROACH)

Information collection, Information processing, Autonomous deployment

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal Of Management & Information Technology

Vol . 10, No 8

editorsijmit@gmail.com

www.ijmit.com

1. INTRODUCTION

The Internet of Things (IoT, for short) is a heterogeneous, mixed and uncertain ubiquitous network. It is booming in the field of modern intelligent service, such as ecological protection, energy conservation & emission reduction, food security, etc. The autonomic cognition and intelligent decision-making mechanism is the core to achieve intelligence for IoT. In recent years, cognition and cooperation have become the hot spot in related research domain. Since Dr. Mitola [1] proposed the concept of cognitive radio, cognitive radio network and cognitive network attracted a large number of researchers, and they achieved many research achievements, which promoted the development of the network intelligence research greatly. In these studies, cooperation thought is often used to implement the intelligence of heterogeneous network, multiple path user network, multi-agent network, multi-hop network, biological neural networks, autonomous system and other intelligence network.

In recent years, with the rapid development of IoT, the increasingly complex user demand put forward higher requirements to resource sharing and collaborative work between the nodes in the network. CIoT possess self-organizing, self-sensing, self-configuration and self-optimization features to meet the needs of the current network,which will also increase the difficulty of network management. Though collaboration between nodes are in the concept of “all for one, one for all”, in fact, existing studies have shown that plenty of nodes just want to get the service provided by other nodes in the network rather than willing to contribute to other nodes [2]. There are multiple autonomous domains in the CIoT, while, with the limited notes resources such as processing capacity, battery power and so on, different autonomous domain nodes may have different goals, so, inevitably some selfish nodes exist. As a result, how to detect selfish node in the network and encourage the cooperation, so as to ensure the performance of network is one of the significant issues to be addressed in CIoT.

2. RELATED WORKS

According to the questions of selfish nodes in the network, the reputation mechanism is a relatively ideal solution. Reputation is often cited as the standard of economic and social activities, such as individual credit archives, credit card and so on. The credibility of the network is the early solution to help people build a trust relationship on the Internet. It does not need to build costly regulatory agencies to manage the cooperation between people. The scheme through credibility to establish trust relationship is emerging on the Internet. Reputation mechanism has a favorable reputation management system, safe network environment, convenient communication channels, so it is being pursued by more and more people. The basic idea of reputation-based incentive mechanism assesses the trust of nodes according to their credibility which is the basis for motivate decisions. When all nodes in the network are able to participate in the cooperation to achieve optimum performance of the entire system, then each node will be able to derive the corresponding optimal returns. By observing and monitoring cooperative behavior between nodes to punish uncooperative nodes, to ensure that all nodes are able to cooperate actively. Watchdog [3] and Pathrater [4] mechanism were proposed earliest, used to solve network problems of routing error caused by selfish nodes. Watchdog is to detect inappropriate behavior nodes, where each node monitors its next hop node after sending or forwarding a packet: if there is no forwarding in the next hop node, it indicates some problems; on the basis of the detail collected information of the nodes, Pathrater assesses trust level of each path, trying to avoid the potentially problematic nodes.

At present, the distributed trust model is a hot research field in trust management, grid computing, P2P [5], sensor networks [6], mobile computing and pervasive computing and other fields have corresponding research. The classic trust management techniques include Trust model based on statistics (TMBS, for short) [7], Pervasive Trust Management Model (PTM, for short) [8], Hassan Model [9], Dirichlet trust algorithms [10], fuzzy trust model [11] and Cloud model trust algorithm [12], etc. [13] proposed a reputation model based on Markov chain model for the vehicle in Ad Hoc (VANETs, for short) Networks, in the model, each vehicle can monitor and update its trust degree operating based on the behavior of the neighbor vehicle. According to malicious nodes in the P2P network, [14] analyzed Peer Trust-Like mechanism, gave the corresponding mathematical description, and calculated the trust value by using formal similarity between nodes. [15] proposed a trust evaluation model that will use the path similarity and information similarity to evaluate the credibility of information and information source nodes, as a feedback, adaptive network node's trust value. Literature [16] proposed an email reputation management system-CARE based on mutual cooperation between the autonomous domain, which effectively improved the reliability and efficiency of e-mail systems. [17] designed a distributed collaborative reputation mechanism of trustworthiness published by autonomous systems, it has been shown to effectively contain autonomous' bad behaviors, and hence improve the overall security of the inter-domain system. For selfish nodes in the mobile ad-hoc network reduce multi-hop connection, to enhance the cooperation of the data from the source node to the destination node, literature [18] controls the relay nodes by the watchdog detection mechanism to forward packets correctly and gather information about potential selfish nodes to reduce selfish behavior of nodes and increase the capacity of the effective routes. Literature [19] was used to optimize end-to-end high latency and frequent disconnection of communication links which present at the delay tolerant networks (DTNs, for short), to develop an analytical model based on trust, which carry on dynamic trust management for selfish nodes and malicious nodes. The model reduces the deviation of dynamic changing network environment, weights the cost of the transmission of information and enhances the efficiency of information transmission.

According to the characteristic of CIoT, this paper analyzed the advantages and disadvantages of the Account-based Hierarchical Reputation Management (ARM, for short) trust model [20], and proposed C2R. Based on ARM trust model, the direct and indirect evaluations are weighted to calculate the reputation value of nodes. Taking the time factor into account, the penalty value to constrain the node with too high reputation value is introduced. Meanwhile, based on original model, response module is added to implement the node classifying and appropriate incentives according to reputation value. Finally, in order to enhance the scope of the program application, we introduce a multi-domain cooperation mechanism to make cross-domain evaluation of the nodes more objective and true. The paper is organized as follows. We introduce the conception of CIoT and analyze the ARM trust model in section 1 and 2. In Section 3, We proposed C2R, which improved the calculation method of the nodes reputation, and strengthened the interaction between domains by the introduction of multi domain cooperation mechanism. We carried out experiments to validate the effect of our mechanism, and the experimental results were analyzed in section 4. Finally, the conclusion is presented in section 5.

3. SYSTEM MODEL

3.1 Cognitive Internet of Things

The research work in this paper is based on the topology shown in Figure 1. We consider that the CIoT [20] is a group of autonomous domain $AD_1, AD_2, ..., AD_n$. CIoT is defined as high coupling inside and relatively independent outside. Domain is autonomous domain contains different cognitive nodes (CN, for short), simple nodes (SN, for short) and network links, such as computers, routers, servers, switches, printers, and other equipment.

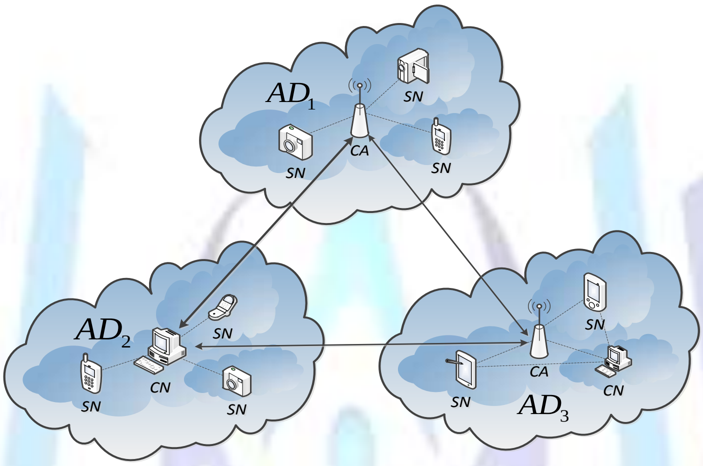

Fig 1: Topology of Cognitive Internet of Things

Autonomous domain can be divided into multiple sub-domain, and the *CN* also known as cognition element relative to the general node with no wisdom are joined to the domain, which can optimize the network performance automatically according to network state. If a domain has multiple cognitive nodes, cognitive nodes can cooperate according to the need. When the cross domain collaboration is needed, specific cognitive nodes which are called cognitive agent (*CA*, for short) will implement the multi-domain cooperation, and a domain can have one *CA* or more.

In the process of information transmission in CIoT, *SN* perceives the external environment information, and sends the information to adjacent *CN* or *CA* through the transmission channel. *CN* perceives network status information and receives the information from *SN*, then sends it to *CA* after initial treatment. *CA* makes appropriate decisions after processed the autonomous domain sensory information which have acquired, collaborates and interacts with other autonomous domains *CA*.

3.2 ARM trust management model

ARM scheme [20] manages Ad Hoc node behavior using cellular network assisted mode in multi-hop cellular network, with the base station as an auxiliary facilities. In order to improve network throughput and long-term effective incentive, ARM proposed reputation management system-RMS for selfish nodes, dynamically incenting the nodes to forward packets. RMS is set in the base station, and there are two main functional modules: reputation management module and account management module. Reputation management module calculates the reputation value of mobile nodes, and each nodes use watchdog mechanism to calculate the reliability of the neighbor nodes and periodically report to the RMS. Here, reliability is used to compute the current reputation value of nodes. Account Management module calculates the cost of network nodes participating incurred and deserved reward: When a node N sends packets, RMS deducts the value from accounts according to the sending number. When forwarding packets, RMS rewards the value to the accounts according to the forwarding number. Dynamic incentives are embodied in different costs with the credibility of nodes, that is, if N has a high reputation value, it only needs to pay a lower fee to RMS.

The advantages are described as follows.

(1) The scheme comprehensively considers the confidence, history, time and other factors to reflect the dynamics of trust relationship.

(2) The model constructs mathematical model to some uncertain factors, introducing the trust factor, historical factor, and time factor, which is the most distinguishing feature comparing to other models.

(3) The model has better dynamic adaptability, with certain sensitivity and strong ability to resist malicious behavior.

(4) Used in the model are some simple arithmetic operations, with no complicated iterative calculation, so the model has fast convergence speed and better scalability.

The disadvantages are described as follows.

(1) The model cannot solve fraudulent behavior between entities in the recommended for the benefit of each other, and it is assumed that the presenter with high trust couldn't provide unreliable recommendation.

(2) The computation of recommending trust value believes only neighbor node and doesn't consider autonomous domains' reputation, so the calculated trust cannot represent the overall situation.

(3) The lack of punishment for bad behavior selfish nodes, leading to only get reputation of the nodes but can't promote selfish nodes forwarding data eventually.

For the advantages and disadvantages of the existing trust management model, we present our improved program in the next part.

4. C2R SCHEME AND ALGORITHM

Obtaining corresponding reward by users forwarding packets, existing trust evaluation model based on node credibility can solve the problem of indulgence node behavior, so as to allocate network resources dynamically, limit bad behaviors of nodes and share network service fairly. However, calculation method of node reputation value depends greatly on the views of nodes with high reputation value, so it is easy to be influenced by these nodes, leading to subjective bias. So we propose our improved plan to promote nodes cooperation between domains and motivate nodes to forward packets.

In the CIoT, all kinds of nodes, such as laptops, smart phones, printers, routers, etc form an autonomous domain in a certain range. The autonomous domain can realize the connection by border gateway or the cognitive nodes (as a repeater) of neighbor domain. In order to adjust the accuracy of the assessment of the credibility of the nodes, we add node time decay factor to the calculation process. In autonomous domain, we only consider the connection in autonomous domain nodes through cognitive nodes, and by which, implementing dynamic management to resources and motivating collaborative forward. When evaluating the need for cross-domain, it needs to cooperate in multi-domain to gain trust relationship between autonomous domains to ensure the node cross-domain evaluation more accurate.

In Figure 2, our proposed C2R includes four main modules: monitor module, reputation management module, pricing module and response module.

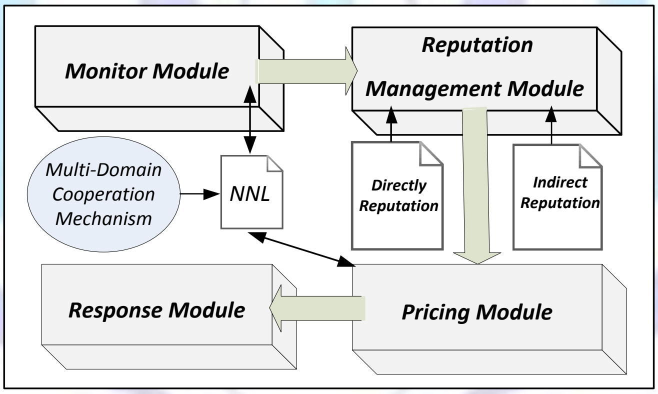

Fig 2: Module of C2R system

4.1 Monitor module

This module mainly collects information on neighboring nodes. Each cognitive node possesses and maintains neighbor nodes' list (*NNL*, for short). Table 1 gives a glimpse of *NNL* that contains the Neighbor Node ID, Reputation Value, Reputation Pricing Information, Account, Domain ID, and Time Stamp. With T_p as the period, cognitive node query and update the information of neighbor node from other cognitive nodes, and T_p can be adjusted according to the degree of network change.

Table 1. Neighbor nodes' list

ID	Reputation value	Pricing	Account	Domain ID	Time
Node(a)	RV(a)	RV(a)	AC(a)	AD_1	T_1
Node(b)	RV(b)	RV(b)	AC(b)	AD_1	T_2
Node(c)	RV(c)	RV(c)	AC(c)	AD_2	T_3

…	…	…	…	…	…

CNs used two counters: *RF* and *HF*, to monitor all neighbor nodes in the domain and observe the behavior of their forwarding. Figure 3 shows that, if node ***i*** send the packet to the node ***n***, node ***j*** will be as an intermediate node, meanwhile, ***i*** will forward the packet to ***a***, ***b***, ***c***, and ***j***. These nodes copy the packets to their cache; every one increases a packet, and the counter *RF* is plus 1.

Within the time T_p, each node sends a packet, and the counter *HF* is plus 1.When ***j*** receives packets, in general, in order to increase the value of *HF*, no matter from which node are the packets forwarded, they will be forwarded. is the number of forwarding packets requested by node ***i*** to node ***j***. is the number of forwarding packets for ***i*** by ***j***. The two values are updated once every.

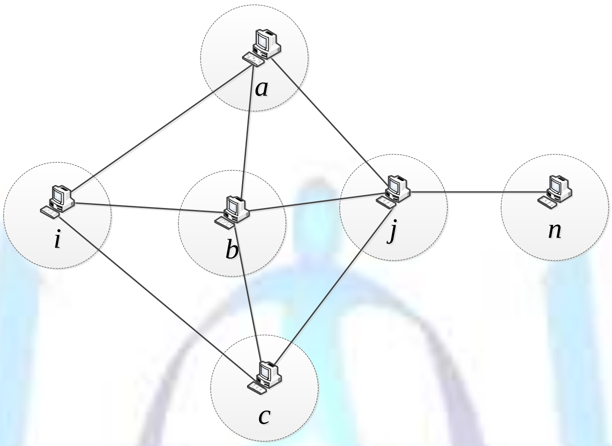

Fig 3: Structure of monitor module

Monitor module calculates the node activation value based on the existing conditions, so is calculated by formula (1).

$$\varphi_i(j)=\frac{HF_i(j)}{RF_i(j)} \tag{1}$$

It implies that, in the period T_p, the more packets ***j*** forwards, the higher activation value it gets. Monitor module will calculate $\varphi_i(j)$ and send the calculated value to reputation management module of other cognitive nodes.

4.2 Reputation management module

Each cognitive node reports its monitor value to reputation management module periodically. In the period, there will be multiple cognitive nodes to observe a specified node, and send the observed results to this module. We weigh the direct reputation and indirect reputation to reduce risk, and by punishing to reduce subjective bias. Nodes' reputation value consists of direct reputation value, indirect reputation value and penalty value. The calculation process is showed as formula (2).

$$RV(n)=\alpha RV_{dir}(n)+\beta RV(n)_{indir}-\omega P(n) \tag{2}$$

Here, $\alpha+\beta=1,\ 0\le\omega\le1$. Direct reputation is the reputation of a node according to the direct interaction experience of the subject and object, collected by monitoring module, which takes the time for the effects of node reputation value calculation into consideration. Due to the dynamic change of CIoT nodes, in order to improve the accuracy of the evaluation and dynamic adaptability, we divide a period of time into several time interval, that is $t_1,t_2...,t_n$. The time frame length can be determined based on the specific application scenarios, and its time decay formula is:

$$g(k)=g_k=\rho_{fade}^{n-k},\rho_{fade}\in(0,1)\cap k\in[1,n] \tag{3}$$

ρ_{fade} is time decay rate, which means, the farther the distance from the current time, the smaller the reference value. So direct reputation value is calculated as:

$$RV_{dir}(n)=\frac{\sum_{i\in S_N\cup(\varphi_i(n)>\theta)}\varphi_i(n)\cdot g_k\cdot RV_{indir}}{\sum_{i=1}^{n}\varphi_i(n)\cdot g_k} \tag{4}$$

Here, ***i*** is the neighbor node of ***n***, is the collection of neighbor nodes, provide the reputation value of monitor nodes. θ is reliability threshold and the behavior of the node below the threshold would be considered bad.

Penalty value can be understood as, if node uses its reputation value in fraudulent transactions, causing fluctuations, then it will receive the corresponding punishment. The penalty value is calculated as follows:

$$P_t = \frac{\sum_{k\in T_k} g_k \max(0, RV_{indirt}{}^{k}(i,j) - RV_{dirt}{}^{k}(i,j))}{\sum_{k\in T_k} g_k} \qquad (5)$$

In the equation (5), $RV_{indirt}{}^{k}(i,j)$ is the reputation value of node ***j*** when the request node ***i*** pools all the nodes which participate assess during the period of time *k*. $RV_{dirt}{}^{k}(i,j)$ is the direct reputation value of node ***j*** assessed by node ***i*** in the same period.

Finally, according to the different autonomous domains of environment, using formula (2), we will get the nodes reputation value that will be sent to the reputation pricing module.

4.3 Pricing module

In order to avoid equal treatment of each node, pricing module takes a different pricing value depending on different node reputation value. The style of dynamic pricing maintains the fair of nodes, and effectively avoids the selfish behavior of nodes.

In this model, the pricing are based on the reputation table of cognitive nodes, the specific calculation is as following formula (6).

$$M(n) = \gamma / RV(n) \qquad (6)$$

γ is a continuous weight, *M* is the cost spent on each packet transmission. The higher the reputation value of the node is, the lower the transmission cost. And cognitive node creates a virtual account for each user.

In Table 1, Cognitive node assigns a fixed virtual currency to each new node into the network. When a node ***n*** send packets to other nodes, the cognitive nodes will deduct a certain amount of virtual money from the account of the node ***n***, denoted as $M_l(n)\cdot RFS_l(n)$,in which, $RFS_l(n)$ is the packets number of node ***n*** sending to the neighbor in the period of T_p, implies the start time of each period, such as $t_0, t_0+T_p, \ldots, t_0+mT_p$. If the node ***n*** helps other nodes to forward data packets, the account of node ***n*** will increase $\gamma\cdot HFS_l$, in which, γ is the continuous reward of node ***n*** forwarding data packets, HFS_l is the number of node ***n*** forwarding data packets in the period T_p , so account of the node ***n*** is calculated by formula (7).

$$AC(n) = sum - \sum_{l=t_0}^{t_0+mT_p} M_l(n)\cdot RFS_l(n) + \gamma\cdot \sum_{l=t_0}^{t_0+mT_p} HFS_l \qquad (7)$$

Forwarding nodes do not need to pay for the next hop node, and the node account can be negative, of course, only the node with positive account can forward packets.

4.4 Response module

The module is set in cognitive node, which will classify the node via perceiving the level of reputation value and take appropriate measures. Response modules need to design the observation time and decide the current state of the node based on the reputation value. We use a threshold μ to identify whether the node is "cooperation" or "selfish." Once the node is identified as selfish nodes, it will enter a period of punishment, during this time, it will unconditionally forward packets until it restores its reputation by cooperation. Penalty time *T* is:

$$T = \begin{cases} \dfrac{\mu - RV}{\mu}\times T_0, & 0 \le RV < \mu \\ 0, & \mu \le RV \le 1 \end{cases} \qquad (8)$$

In formula (8), μ is a subjective threshold, T_0 is a benchmark to punish time. When the reputation value is greater than or equal to the threshold value, the node will not be punished; otherwise, the punished time will be set by the ratio between *RV* and μ .

Corresponding module involves in the route discovery and route selection. The routing with the best reputation and no selfish node will be given priority. Response module obtains the reputation value report by updating reputation management module, checks the node status of the credibility table, and notifies other nodes in the network through cognitive nodes.

4.5 Multi-Domain cooperation mechanism

In certain circumstances, as shown in Fig.1, if cognitive node collaboration within a single autonomous domain can't satisfy the node reputation evaluation criteria, multi-domain cooperation mechanism to make decisions will be considered. In the process of multi-domain cooperation, each *CA* or *CN* need to maintain their *NNL* in the domain and update the content related to reputation. We assume that they will correct processing about the credibility of the data, and has used the encryption mechanism to ensure that the integrity of reputation management information between domains. We make the $C=(D,V)$ is CIoT, in which, $D=\{d_1,d_2,\ldots,d_m \mid m\in N\}$ is the autonomous domain of CIoT. $V=\{v_{d_id_j} \mid d_i,d_j \in D\}$ is the direct trust relationship between autonomous domain d_i and d_j ,the reliable value $DR_{d_id_j}$ is from d_i to d_j ,$Trust_{d_id_j}^{path}$ is the trust route from the autonomous domain d_i to d_j ,which satisfies the condition that $DR_{d_id_j}\geq 0$, $d_i \neq d_j$. In which the cognitive nodes only visit the node from trusted domain, and we can conclude that:

$$DR_{d_id_j}\begin{cases}\dfrac{e_{d_id_j}-w_{d_id_j}}{e_{d_id_j}+w_{d_id_j}} & ,e_{d_id_j}+w_{d_id_j}\neq 0\\ DR_{d_id_j}^{re} & ,e_{d_id_j}+w_{d_id_j}=0\end{cases} \tag{9}$$

In the equation (9), $e_{d_id_j}\geq 0$ and $w_{d_id_j}\geq 0$ respectively are effectiveness and wastage from d_j to d_i . If $e_{d_id_j}+w_{d_id_j}\neq 0$, the nodes in d_i and d_j occur transactions, $DR_{d_id_j}$ is the direct reputation value for d_i to d_j ; else , among d_i and d_j exist a trust path, d_i will be chosen through the path of the most trusted domain to d_j ,and $DR_{d_id_j}$ is the minimum reputation value on this path. As shown in Figure 4, the best route from AD_1 to AD_7 is $AD_1\rightarrow AD_4\rightarrow AD_6\rightarrow AD_7$, concludes $DR_{d_1d_7}=0.2$.

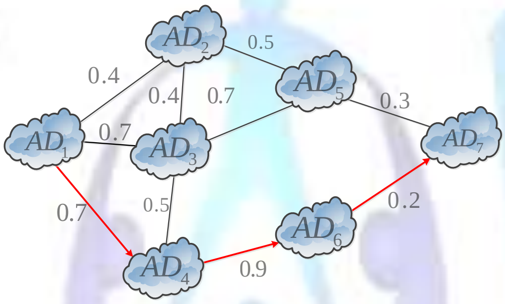

Fig 4: Calculation autonomous domains' reputation by route

Autonomous domain reputation value is stored in the *CA*. When nodes need cross-domain reputation evaluation, we can consider that the credibility of the evaluation value includes the domain and inter-domain evaluation value. Such as the node ***i*** in autonomous domain AD_m , the reputation assess of which is $RV_{d_m}(i)$,the node ***j*** in the autonomous domain AD_m also has the reputation assess of the node ***i*** is $RV_{d_n}(i)$,that is, the reputation value of the node ***i*** is:

$$RV(i)=RV_{d_m}(i)\cdot[DR_{d_md_n}RV_{d_n}(i)] \tag{10}$$

Through multi-domain cooperation mechanism, we can get the trust relationship between autonomous domains, making inter-autonomous domain node reputation evaluation is more objective and accurate.

5 Experimental results and analysis

5.1 Simulation settings

To evaluate the performance of our improved scheme, we use NS2 network simulation tools and LINUX operating system to simulate. Assumes that, in the autonomous domain, messages from the cognitive nodes are accurate, reputations are reliable and don't attack legitimate nodes. Four indicators are used in the simulation process: routing effective throughput [23] the actual effective throughput [24], the number of lost packets and node reputation value. Routing effective throughput means the ratio of the received packets number in the destination node with the sent packets number in the source node in the routing layer. Real effective throughput means the ratio of the received packets number in the destination node with the number of sent packets in the source node in the application layer. The number of lost packets refers to the sum of packets discarded by selfish nodes in 20 simulation processes, the node reputation value refers to all the nodes change during the simulation experiments. In the experiments, we only consider the fixed range and use a certain amount of mobile cognitive node to reflect the CIoT, and each node can act as a server, a client or a router at the same time. The simulation parameters are shown in Table 2.

Table 2. Simulation parameters

Parameters	Value
MAC layer protocol	IEEE802.11
Topology range	1000m×300m
Node number	50

Node movement speed	1-20m/s
Signal coverage radius	250m
Transmission model	Two-Ray Ground Reflection
Business Type	CBR
Packet size	512bytes
Data packet transfer rate	4pkt/s
Max number of connected	20
Monitor cycle()	10s
Reputation threshold()	0.5

In simulation experiment all the nodes as the cognitive nodes in CIoT, namely wisdom nodes. The initial position of each node is random, and the direction and path are random. Simulation of 20 times, each time the 300 s, 10 source nodes and destination nodes in every 10sare randomly selected, so that each node has a chance to send and receive packets. Wherein the proportion of selfish nodes are 0-60%.Selfish node packet loss rate of 0.7, Experimental scene graph shown in Figure 5.

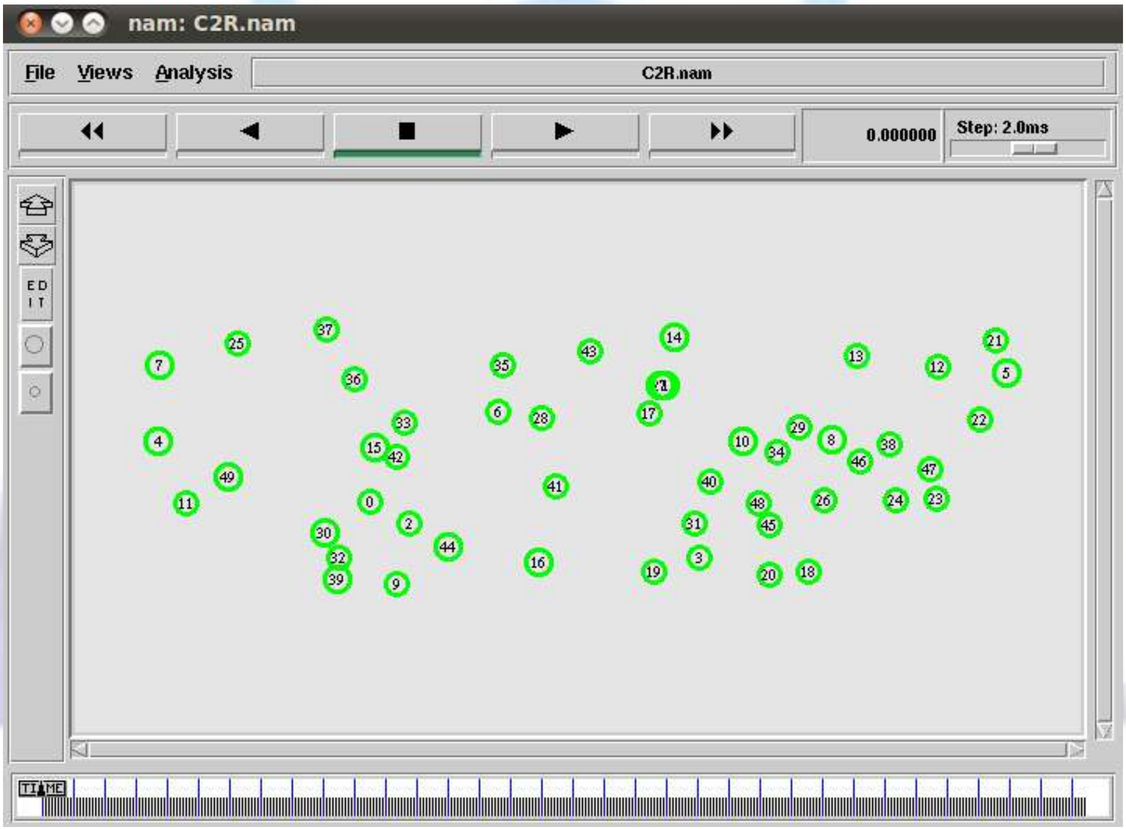

Fig 5: NS2 simulation experiments scene

5.2 Routing effective throughput

Figure 6 illustrates the differences of routing effective throughput between existing schemes and C2R by changing number of selfish nodes. Since only considering the reception condition of sent packets after establishing the routing, the cost of establishing the network routing is not counted. Adjacent nodes exchange the reputation value between each other, and the establishing of routing avoids selfish nodes, so the actual effective throughput in this scheme is higher. When the number of selfish nodes is 60%, routing effective throughput of the C2R reaches 52.7%.And we can see from the curve, with the increase of selfish nodes, the throughput in our solution fell more slowly and relatively stable.

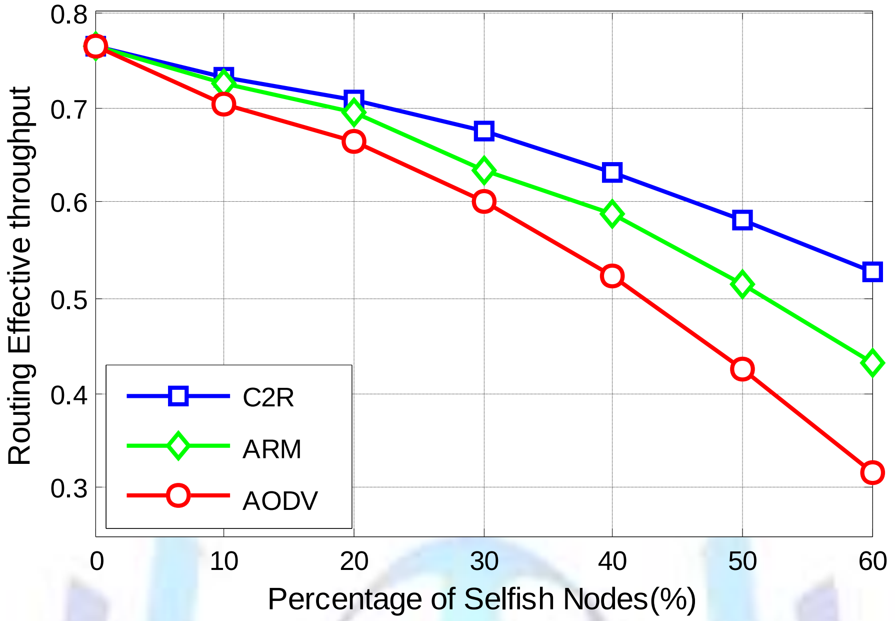

Fig 6: Routing effective throughput along with the change of selfish node number

5.3 Actual effective throughput

Figure 7 illustrates the differences of actual effective throughput between existing schemes and C2R by changing number of selfish nodes. C2R perfects the formula of reputation value in ARM node, while taking advantage of multi-domain coordination mechanism for inter-node reputation evaluation made improvements, inspired forced selfish nodes to forward packets, increased network utilization, so the actual effective throughput is better improved.

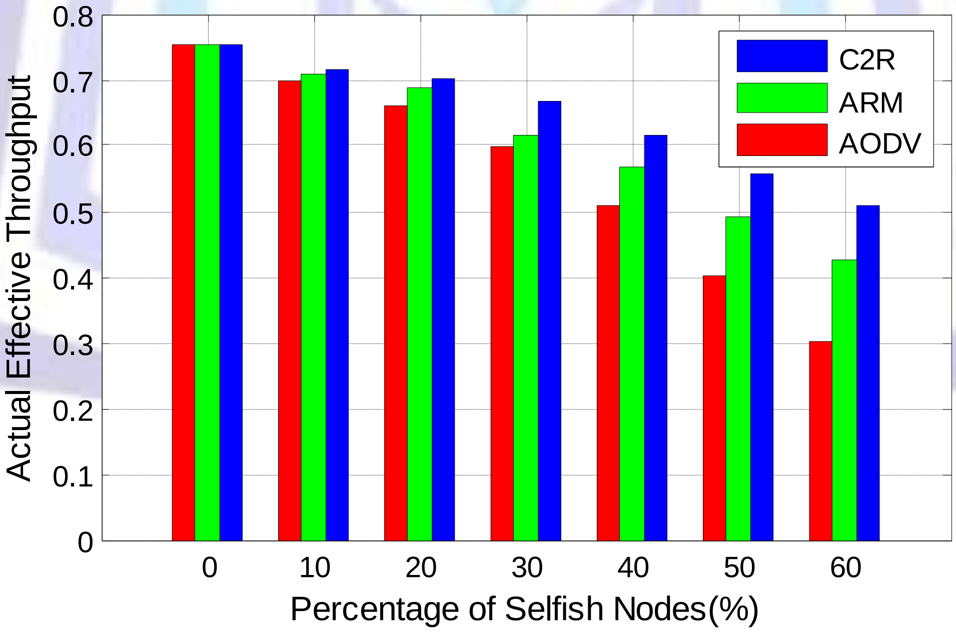

Fig 7: Actual effective throughput along with the change of selfish node number

5.4 Packet dropout

Figure 8 illustrates the differences of the lost packets number between existing schemes and C2R by changing number of selfish nodes. Since the response module prompted low reputation value selfish nodes to forward packets mandatory, and effectively control the packet loss rate.

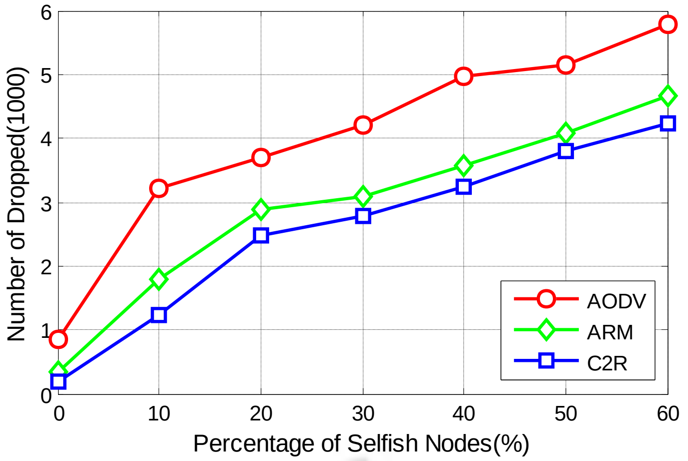

Fig 8: Packet loss rate along with the change of selfish node number

5.5 Node reputation value

Figure 9 shows the compare of different reputation value of nodes when the simulation time is between 150s and 300s, and the selfish nodes in C2R mechanism are 60%. We can conclude that at the end of the experiment, the change of the original high reputation value node is not obvious, but reputation value of those nodes with lower value is improved obviously.

Their reputation value also has a certain improvement because the selfish nodes are forced to forward packets. From the figure we can see that in 150s quite a number of nodes reputation value is below than 0.5, when the simulation proceeds to 300s, only reputation value of a small parts is below 0.5.It can be proved that our incentive scheme for node forwards the packet has a good effect, and the simulation makes large number of nodes reach a given requirement.

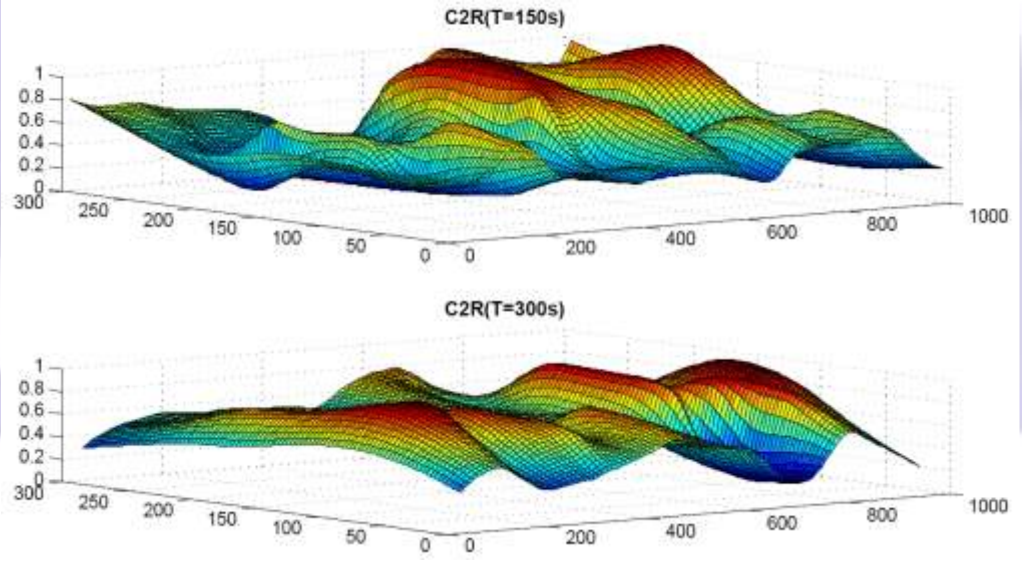

Fig 9: C2R node reputation value comparison in different periods

6 Conclusion

Based on the related research of IoT, this paper strives to improve its intelligent property, and optimize the CIoT in order to realize the maximization of self-management. For there may be selfish nodes in the CIoT, we propose Cognitive Internet of Things-oriented Multi-Domain Cooperation Dynamic Incentive Mechanism, and build the related model. Based on the existed model of the ARM reputation evaluation, we improve the methods to the node reputation evaluation, achieving the reputation of node across autonomous domain of credit assessment by the thought of multi-domain cooperation, enhancing the objectivity and credibility of the node assessment. Finally, the simulation results compares the routing effective throughput, the actual effective throughput, the number of lost packets and the node reputation value between our scheme and existing ARM scheme. The result shows that the four indicators have been improved significantly, and the inter-node and inter-domain collaboration behaviors have been implemented in the network.

Of course, C2R also has some defects. Because this experiment is established in relatively ideal circumstances, without considering node by malicious attacks, such as Trojan virus can cause the node to send a lot of useless data form DDOS attacks [25], the next step research will focus on how to find harmful neighbor node, and bring risk factors into reputation evaluation calculation.

ACKNOWLEDGEMENTS

This work was supported by Project of Natural Science Foundation of China (No. 61142002, U1204614, 61003035), Natural Science Foundation of Henan Province Education Department (No.2010A520018), Key Project of Science and Technology Department of Henan Province (No.112102210187) and Research Funds for Doctor of Henan University of Science and Technology.

REFERENCES

[1] Mitola, J. 2009. Cognitive radio architecture evolution. In Proceedings of the IEEE.

[2] Ciobanu, R. I., Dobre, C., Dascalu, M., Trausan-Matu, S.and Cristea, V. 2014. SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks. Journal of Network and Computer Applications 41 (May. 2014), 240-249.

[3] Wahab, O. A., Otrok, H., and Mourad, A. 2014. A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles. Computer Communications 41 (Mar. 2014), 43-54.

[4] Ko, J., Seo, J., Kim, E. J. and Shon, T. 2012. Monitoring agent for detecting malicious packet drops for wireless sensor networks in the microgrid and grid-enabled vehicles. International Journal of Advanced Pobotic Systems, 9 (May. 2012).

[5] Wang, M., Tao, F., Zhang, Y. and Li, G. 2010. An adaptive and robust reputation mechanism for P2P network. In Proceedings of ICC.

[6] Abumansoor, O. and Boukerche, A. 2011. Towards a secure trust model for vehicular ad hoc networks services. In Proceedings of GLOBECOM.

[7] Zekri, M., Jouaber B.and Zeghlache, D. 2010. On the use of network QoS reputation for vertical handover decision making. In Proceedings of GLOBECOM Workshops.

[8] Mármol, F. G. and Pérez, G. M. TRMSim-WSN. 2009. Trust and reputation models simulator for wireless sensor networks. In Proceedings of ICC.

[9] Jameel, H., Hung, L. X., Kalim, U., Sajjad, A., Lee, S. and Lee, Y. K. 2005. A trust model for ubiquitous systems based on vectors of trust values. In Proceedings of Seventh IEEE International Symposium on Multimedia.

[10] Fung, C. J., Zhang, J., Aib, L. and Boutaba, R. 2011. Dirichlet-based trust management for effective collaborative intrusion detection networks. IEEE Transactions on Network and Service Management 8 (Jun. 2011), 79-91.

[11] Schmidt, S., Steele, R., Dillon, T. S. and Chang, E. 2007. Fuzzy trust evaluation and credibility development in multi-agent systems. Applied Soft Computing Journal 7 (Mar. 2007), 492-505.

[12] Wang, S., Zhang, L., Wang, S. and Qiu, X. 2010. A cloud-based trust model for evaluating quality of web services. Journal of Computer Science and Technology 25 (Nov. 2010), 1130-1142.

[13] Gazdar, T., Rachedi, A., Benslimane A. and Belghith, A. 2011. A distributed advanced analytical trust model for VANETs. In Proceedings of GLOBECOM.

[14] Wang, M., Xu, Z., Zhang Y. and Zhang, H. 2011. Modeling and analysis of Peer Trust-like trust mechanisms in P2P Networks. In Proceedings of GLOBECOM.

[15] Wang, X., Govindan, K. and Mohapatra, P. 2010. Provenance-based information trust worthiness evaluation in multi-hop networks. In Proceedings of Global Telecommunications Conference.

[16] Xie, M. and Wang, H. 2010. A collaboration-based autonomous reputation system for email services. In Proceedings of INFOCOM.

[17] Hu, N., Zou, P. and Zhu, P. 2010. Reputation-Based collaborative management method for inter-domain routing security. Journal of Software 21 (Mar. 2010), 505-515.

[18] Rodriguez-Mayol, A.and Gozalvez, J. 2014. Reputation based selfishness prevention techniques for mobile ad-hoc networks. Telecommunication Systems 57 (Oct. 2014), 181-195.

[19] Chen, I., Bao, F., Chang, M. and Cho, J. 2014. Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Transactions on Parallel and Distributed System 25 (May. 2014), 1200-1210.

[20] Shen, H. and Li, Z. 2008. Arm: An account-based hierarchical reputation management system for wireless ad hoc networks. In Proceedings of Distributed Computing Systems Workshops.

[21] Zhang, M., Zhao, H., Zheng, R., Wu, Q. and Wei, W. 2012. Cognitive internet of things: Concepts and application example. International Journal of Computer Science Issues 9 (Nov. 2012), 151-158.

[22] Gopalan, R., Li, R.and Chellappa, R. 2014. Unsupervised adaptation across domain shifts by generating intermediate data representations. IEEE Transactions on Pattern Analysis and Machine Intelligence 36 (Nov. 2014), 2288-2302.

[23] Cohen, R.and Raz, D. 2014. Cost-effective resource allocation of overlay routing relay nodes. IEEE-ACM Transactions on Networking 22 (Apr. 2014), 636-646.

[24] Lashgari, S. and Avestimehr, S. 2013. Timely throughput of heterogeneous wireless networks: Fundamental limits and algorithms. IEEE Transactions on Information Theory 59 (Dec. 2013), 8414-8433.

[25] Yu, S., Tian, Y. and Guo, S. 2014. Can we beat DDoS attacks in clouds? IEEE Transactions on Parallel and Distributed Systems 25 (Sep. 2014), 2245-2254.

Author' biography with Photo

Tenghao Li, he was born in Henan Province, China in 1988. He received the B.E. degree in 2012. He is currently studying as a M.E. in Information Engineering College, Henan University of Science and Technology. His research interests include IoT, Cluod computing and QoS routing.

Ruijuan Zheng, she was born in Henan Province, China, in 1980. She received the D.E. degree from Harbin Engineering University in 2008. She is currently an associate professor of Information Engineering College, Henan University of Science and Technology. Her research interests include autonomic computing, IoT system, bio-inspired computer network security theory and technology, etc.

Ying Li , she was born in Henan Province, China in 1991 . She received the B.E. degree from Henan University of Science and Technology in 2013. She is currently studying as a M.E. in Information Engineering College, Henan University of Science and Technology, China. She is mainly engaged in IoT, QoS routing and Machine Learning.