Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July, 2021: 7914-7924

Research Article

Trust based Lightweight Assailant Detection in Cloud-Assisted WSN

[1]Antony Joseph Rajan D, [2]Naganathan E R

Abstract

Trust Management (TM) is an effective way to solve the intrusion problems occurred in WSN. Trust based Lightweight Assailant Detection Scheme (TLADS) is proposed for identifying and isolating the malicious sensor nodes in cloud-assisted WSNs. Here recommendation trust computation using the node confident level is computed by using decentralized trust computation process. Hence a trust value for each and every node is computed and highly trustable nodes are selected for the route formation to the cloud server. Later cloud level integrity procedure is carried out for selecting the trustable cloud servers by using third party auditing process since the cloud server is made as public. TLADS scheme can construct paths consisting of highly trusted nodes to the cloud, subject to a desired path length constraint. The simulation result shows that TLADS mechanism successfully avoids intrusions, even when a large portion of the data frames forwarded over the network.

Keywords: Recommendation trust, Sensor nodes, Cloud Server, Third-party auditing, Key generation centre.

1. Introduction

Wireless Sensor Networks (WSNs) are centralized network with distributed sensors placed at different locations and the data can be passed through multi-hop manner, here more than hundred nodes are used with sensing capacities. Sensor nodes are usually deployed in not attend-able areas for performing difficult tasks [1]. A non-network node receives the relayed packets and decides whether to connect with the network [2]. WSN plays a major role in the fields such as smart city [3], battlefield surveillance, healthcare monitoring, interference recognition, emergency response with Internet of Things (IoT) [4] etc. Though the network system is highly prone for the security attacks due to the remote characteristics and less link controlling approach is followed in some kind of network topology [5]. For example, dispersed cooperation system, lack of central authority etc. the nodes are considered to be legitimated one by taking normal nodes characteristics and cryptographic keys for comparison [6]. Since, it causes huge damage for the network.

[1]Research Scholar, SCSVMV University, Enathur, Kanchipuram, India, Email: antonyjosephjmj@gmail.com
[2]Professor, Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, India. Email: ernindia@gmail.com

IoT is an upcoming and promising technology that has developed in recent years. It is defined as the network concept with the physical devices, objects, buildings and other constructions, vehicles etc, embedded with electronic devices, sensors, and network connectivity which were dumped with software that allows the objects to get connected with each other and transfers the data [7]. The IoT leads a constant universal correlation between things and people. However, due to the resource constraints of IoT devices, high computational tasks with huge data storage tasks are handled by the resource enriched cloud model which improves efficiency in results. IoT and Cloud Computing together with a focus on the security issues of both technologies was monitored [8]. Specifically, Cloud Computing and IoT are the aforementioned technologies here the common features are examined and the benefits of their integration was discovered.

2. Related Works

Some of the protocols related to trust based sensor networks and cloud's trustworthiness are discussed here for the common reference.

Trust computation models are mostly efficient for mitigating the internal attacks. Therefore a disparity technique that evaluates direct trust was proposed in [9] which use the hysteresis curve for computing the trust values. The property of hysteresis curve is used here for computing the neighbor node's trust value by considering its forwarding behavior. Recently, trust-based solutions have proved to be more effective to address nodes' misbehavior attacks. Trust and Energy aware Routing Protocol (TERP) was proposed [10] here distributed based trust scheme is used for identify the malicious and selfish nodes and keep them away from the routing. Also TERP follows a composite routing function which involves that encompasses trust, residual-energy, and hop-counts of neighbor nodes in making routing decisions. Energy consumption gets balanced by using this routing strategy among trusted nodes. Beta and LQI-based Trust Model (BLTM) for the WSNs was proposed in [11]. Here initially, energy, data and communication trusts are considered during the evaluation of direct trust. Then, the weights of energy, data and communication trusts are discussed. Finally, a Link Quality Indicator (LQI) method was proposed for accuracy and stability maintenance for trust value of nodes connected with low quality links that presented in the network.

Efficient Dynamic Trust Evaluation Model (DTEM) for WSNs [12] is proposed, which implements accurate, efficient, and dynamic trust evaluation by dynamically adjusting the weights of direct trust and indirect trust and the parameters of the update mechanism. To achieve accurate trust evaluation, the direct trust is computed with the punishment factor that includes energy, data and communication trust along with regulating function. The indirect trust is computed by using recommendation trust obtained from third party. In addition dynamic weights are used to measure the integrated trust which is the combination of direct trust and indirect trust and combining them. In order to evaluate node reputation and trust factor the Exponential-based Trust and Reputation Evaluation System (ETRES) [13] was proposed. Node's behavior is analyzed through ETRES and exponential distribution is used to represent the distribution factor of trust for the nodes. The reliable nodes are determined through their trust value that able to transfer the data without any loss and malicious attacks in sensor network. Uncertainties of nodes can be measured up using entropy theory that computes direct trust.

Quality of Service (QoS) based trust assessment method is one of the trust evaluation models in cloud services. A compliance-based multi-dimensional trust evaluation system [14]

was proposed for measuring the trustworthiness of a Cloud Service Provider (CSP). This system helps Cloud Service Centre (CSC) for selecting the good CSP from the available various service providers which satisfies the preferred QoS necessities. A trust-centric approach [15] based on hypergraph-binary fruit fly optimization was proposed for the identification of trustable and apt CSPs. Trust assessment system for Security and Reputation of Cloud Services (SRCS) was proposed which enables trust evaluation for cloud services to make sure the level of security for cloud-based IoT. This process of context of integrating security and reputation is defined to be SRCS based trust model [16]. This security based trust model employs specific cloud security metrics for measuring the cloud trustworthiness. Also the quality of cloud services are exploited through the feedback ratings of the nodes that evaluate the reputation of a cloud service.

A combination of feedback evaluation component along with Bayesian game model trust evaluation method was proposed [17] for identifying the malicious CSCs efficiently on basis of their feedback ratings. The former determines fake identity centers and latter is used to identify false users along with their feedback. A trust evaluation method for collaborations of data-intensive services is considered in [18]. The relation of implicit trust values present in the data dependencies during services is also considered along with the trust value of individual partner services that calculates the relation of explicit trust values among partner services that have logical dependencies for each other.

3.Proposed Scheme

Trust based Lightweight Assailant Detection scheme is proposed for identifying and isolating the malicious sensor nodes in cloud-assisted wireless sensor networks. Here node confident level is identified by using centralized trust computation process. Here recommendation trust process is applied to identify the trust values for each and every node. Trust based system integrates reputation management, trust-based route discovery, and identification of intrusion based on node behavior. A cloud level data integrity check is done through third party auditing process for the public cloud server. Figure 1 shows the example scenario of cloud assisted wireless sensor network.

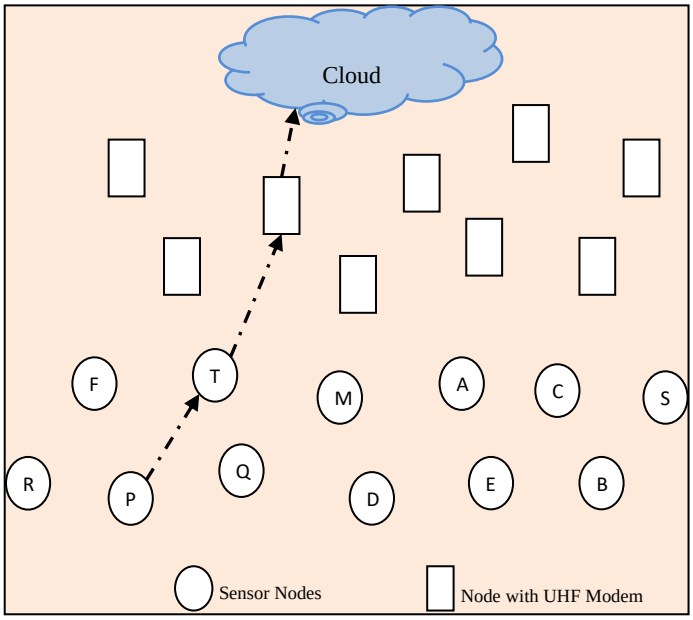

Figure 1: Cloud assisted Network Scenario - Example

(i) Recommendation trust computation

The trust evaluation for each node's is done through recommendation probability of nodes by computing the weight of the node interactions. Recommendation probability measures the recommendation accuracy using the interaction values of node 'P', 'R' and 'S'. At first the direct trust value is computed between the nodes through data forwarding behavior i.e. the confidence value of node P transmits data to R is D1 and node R transmits data to S is D2, therefore D1 = D2 represents the trust value, the node R holds the trust value of (0,1) if D1 = D2 then R holds the belief value '1' and D1!= D2 then R holds the belief value '0'. Equation 1 gives measurement of direct trust values. Direct trust weight is described in figure 2.

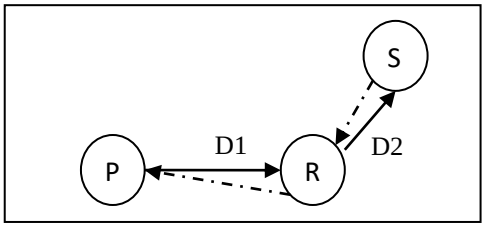

Figure 2: Direct Trust Weight

$$D_{\mathrm{T}(P,\,R)} = \frac{Pkts\ fwd' \rightarrow R}{Pkts\,drop' \rightarrow R + Pkts\,sent' \rightarrow P} \tag{1}$$

Recommendation trust is computed using weighted Dempster-Shafer theory. It measures the recommendation trust accuracy of the nodes. The recommendation probability of the source node and its neighbour nodes are computed, let X_{PR} is a set of neighbours of nodes 'P' and 'R' and the recommendation probability of trust for node 'R' is calculated at 'P' using equation 2.

$$D_P^R(t) = \sqrt{\frac{(\sum_{x \in Xab} DT_P^X(\mathrm{t}) - DT_R^X(\mathrm{t}))^2}{\left|X_{PR}\right|}} \tag{2}$$

From the set of value of direct trust the recommendation weights for the neighbour nodes is estimated, X represents the set of direct trust values obtained for the neighbour nodes and Y represents the recommended trust given for the neighbour nodes, the recommended trust is obtained using equation 3.

$$R_P^R(t) = (1 - \mathrm{D}_P^R(\mathrm{t})) \times \sum_{i \in X_{PR}} (\mathrm{Xi} \wedge \mathrm{Yi}) \Big/ n \tag{3}$$

Here n denotes the sum of number recommendation trust values.

If the Direct Trust (DT) and the Recommendation Trust (RT) identified for the nodes are same then the node is labelled as Trusted Node (TN). If the resultant value seems to be different then the node is considered to be Malicious Node. Table 1 gives the resultant node which is obtained from the DT and RT values.

Table 1: Resultant Nodes

S No	DT (X)	RT (Y)	Resultant Value
1	0	0	TN
2	0	1	MN
3	1	0	MN
4	1	1	TN

Algorithm: Recommendation Probability

Proc (Recommendation Probability)

DT(P) & DT(R) arrays obtained from neighbor_nodes 'P' & 'R'

DT ← 0

RT_count ← 0

For i ← 1 to |N_PR|

$DT \leftarrow \sum DT_{PR} + [(DT\_P) - (DT\_R)]^2$

If $[(DT\_P) - (DT\_R)] < \delta$

Then RT_count ← RT_count+1

$D_{(P, R)} \leftarrow Sqrt(DT/|N\_PR|)$

$RP \leftarrow (1- D_{(P, R)}) \times (RT\_count)/|N_{PR}|$

Close();

Once the trust value is received from the neighbor, the corresponding node updates the neighbour's node trust value. Then the trusted nodes are selected for transmitting the data to the cloud server

(ii) Cloud Level Integrity

By taking the trusted nodes the data is passed to the cloud server. The malicious node cannot able to modify the sensed data. Once the trusted nodes are identified then the sensed information is passed to the cloud server. Commonly cloud server is classified into three

different servers such as private cloud, public cloud, and hybrid cloud (both included public and private). Private cloud is specially designed cloud server that can be used only the individuals or private owned company; and hence the information privacy is guaranteed. But in public cloud or hybrid cloud the CSP seems to be unsecured since it was designed with untrusted third party, therefore the data confidentiality is not protected, example the user's sensitive medical related data can be easily exposed to others CSP's. That is the client information is uploaded to the cloud server directly without processing any encryption method. Therefore, a cloud-assisted WSNs public auditing scheme is composed of cloud server, key generation centre, client, and third-party auditor. Here, the cloud server (the client can upload or download the data) and key generation centre is partially-trusted thing. Third-party Auditor (TA) checks the data integrity of the stored information and the received information from the sensor nodes. Service Provider (SP) sends the secured information to the client by verifying the third party auditing results (True/False).

The key generation Centre (C_{KG}) generates the Partial Private key (PPk) and send this generated PPk to the service provider. Each service provider own's their unique Identity (Id) and the Id is encrypted with the partial public keys ($Id_{(SP)}$).

The TA checks for the correctness of the data pack (D_{frame}, r_i) either the information is TRUE or FALSE with the proof (Pr, D), TA executes the data integrity check for D_{frame}. The Id of the SP and the generated partial private key for the respective SP is primarily taken by the TA. Then TA computes the data integrity 'Do', 'Di' and verifies the resultant value 'R' using the equation 4.

$$\begin{aligned} Do &= D(\mathrm{Id}_{(SP)}, \mathrm{PPk}_{SP,1}) \\ Di &= D(\mathrm{Id}_{i}, \mathrm{PKC}_{KG}, \mathrm{PPk}_{SP,1}, \mathrm{PPk}_{SP,2}) \\ R &= \sum_{i-1}^{k} Do \square Di \end{aligned} \tag{4}$$

Now the third-party auditing checks the resultant value of the data frame 'D' and proves the data with the metrics TRUE or FALSE. The proof is given in equation 5.

$$e(\mathrm{Pr}, \mathrm{D}) = e(\mathrm{Di}.\mathrm{PKC}_{KG} + \mathrm{R}.\mathrm{PK}_{SP,1}, \mathrm{Do}) \tag{5}$$

Thereby the certificates are generated with the TRUE/FALSE report for the particular SP from which the data is accessed.

4. Results and Discussion

The simulation analysis is carried out for the analysis of network performance and efficiency for the proposed mechanism using simulation tool called Network Simulator (NS) version 2 and as called as NS2. It is possible to examine the events in a network scenario discreetly. To assess the network performance we evaluate the packet delivery rate, Average delay, Throughput and Node trust ratio metrics of the network before and after adopting the proposed TLADS scheme in comparison with the conventional schemes ETRES and SRCS. Table 2 gives the simulation parameters that are used for the analysis of network performance.

Table 2: Simulation Metrics

Parameter's	Value
Traffic model	Constant Bit Rate
Simulation Area	600 x 600m, 600 x 600m
Transmission range	250mts
Antenna Type	Omni antenna
Number of nodes	50
Network Interface Type	WirelessPhy
Channel Type	Wireless channel
MAC	IEEE 802.11
Data_rate	11Mbps

(a) Packet Delivered Rate

Packet Delivered Rate (PDR) is defined as the amount of packets or frames that is delivered to the receiver end or cloud with respect to the sum of packets that is sent by the sender node. PDR is measured using equation 6.

$$PDR = \frac{\sum Pkts\ dlvrd\ Rate}{\sum Pkts\ sent\ Rate} \tag{6}$$

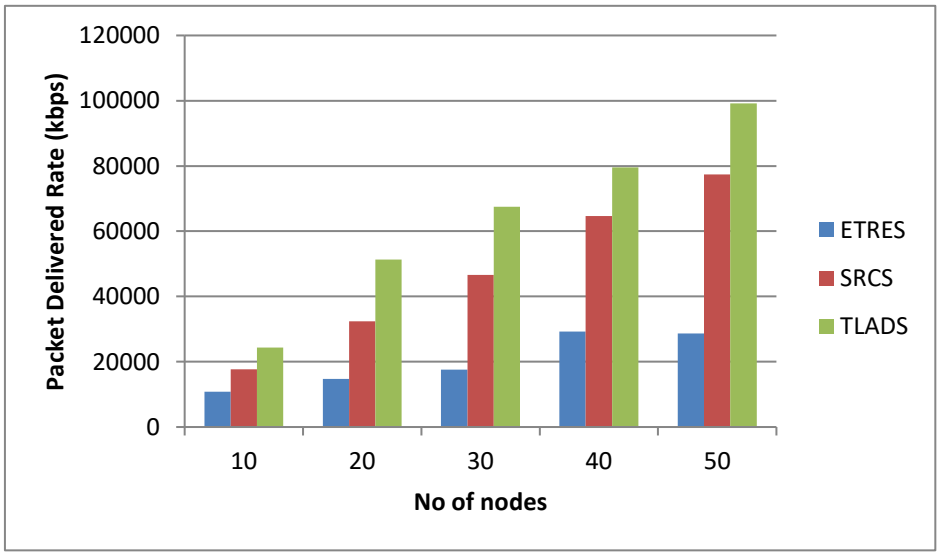

Figure 3: Packet Delivered Rate

From the figure 3, it is clear that the proposed scheme TLADS have delivered large number of packets to the receiver compared to the both conventional protocols such as ETRES and SRCS. Increasing node density is directly proportional to the increase in data packets delivered. This metric proves the better efficiency of the proposed technique.

(b) Average Delay

The average delay is estimated using the difference that occurred in the transmission time of sending packets and receiving packets. This is calculated for all the transmissions taken in the network and evaluated using equation 7. Here n represented for the number of nodes.

$$Delay = \frac{\sum_0^n (Pkt\ Rcvd\ Time - Pkt\ Sent\ Time)}{n} \tag{7}$$

Figure 4 shows the difference between the obtained average values for the proposed TLADS and existing ETRES and SRCS schemes. Proposed TLADS scheme has lower delay values in average computation and it proves that the proposed scheme consumes very less time for processing, transmitting and receiving the packets compared to the other protocols.

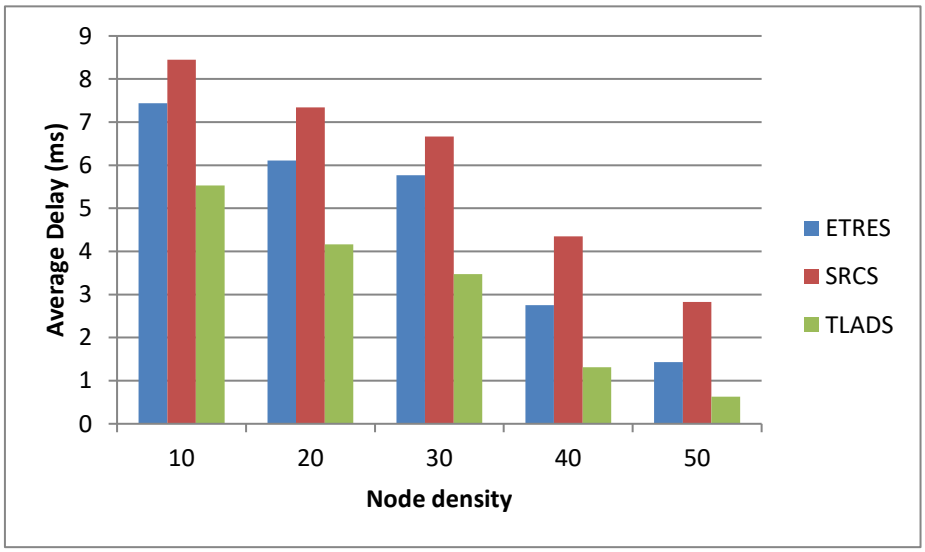

Figure 4: Average Delay

(c) Throughput

Throughput of the network is defined as the successful delivery packets at the receiver end. The sum of number of packets that successfully delivered over the network for every packet that sent successfully. It can be obtained using the equation 8, and n represents the number of nodes.

$$Throughput = \frac{\sum_0^n Packets\ Received(n) * Packet\ size}{1000} \tag{8}$$

The network throughput for the schemes ETRES, SRCS and TLADS are shown in the figure 5. The proposed TLADS scheme has better network throughput when compared with the existing schemes named ETRES and SRCS. Packet delivered rate is directly proportional to the network throughput, i.e. when PDR increases then simultaneously system throughput also increases.

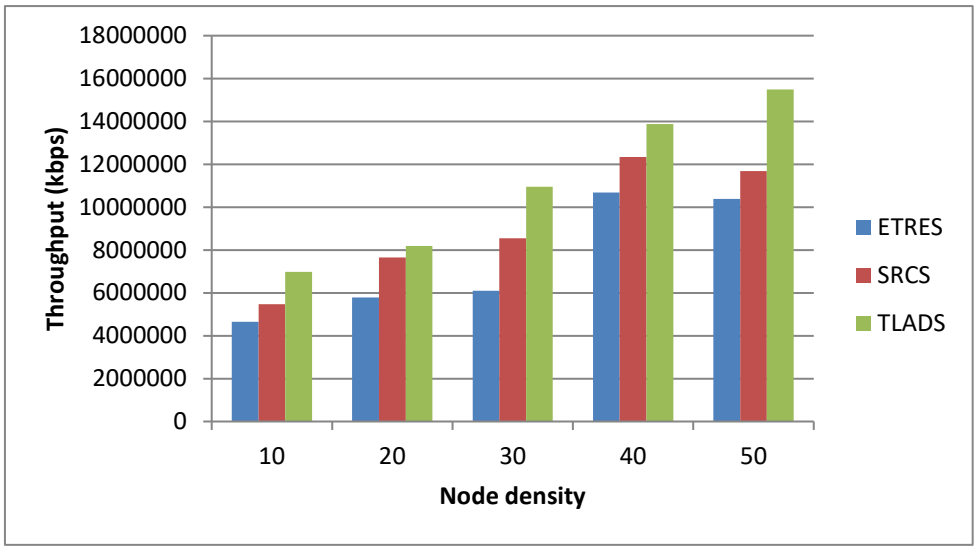

Figure 5: Throughput

(d) Node Trust Ratio (NTR)

The node trust ratio is the ratio of trustable nodes that is selected for the data transmission in the network. Here the NTR is determined in regards of density of nodes that present in the network. Figure 6 shows the node trust ratio for the proposed TLADS and existing SRCS and ETRES scheme. The average NTR that is computed for the TLADS scheme is 0.87 and for the conventional SRCS and ETRES are 0.81 and 0.76 respectively. This shows the TLADS scheme have the capability of selecting highly trusted nodes compared to the existing mechanisms.

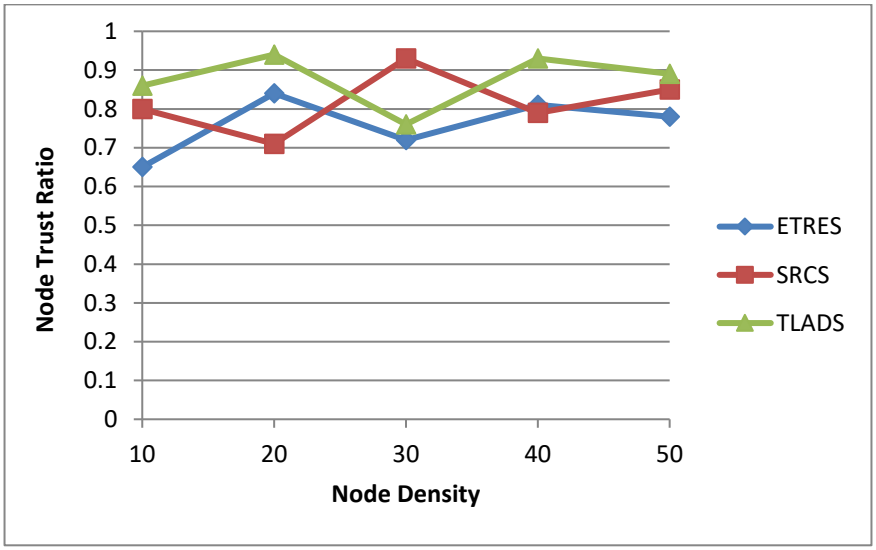

Figure 6: Node Trust Ratio

5.Conclusion

Trust based Lightweight Assailant Detection Scheme is proposed here to detect the trustable sensor nodes and trusted cloud servers in the cloud-assisted WSNs. Here recommendation trust computation using the node confident level is computed by using decentralized trust computation process. So that the trust values for each and every node is identified and the trustable nodes are selected for the route formation to the cloud server. Later cloud level integrity procedure is carried out for selecting the trustable cloud servers by using third party auditing process since the cloud server is made as public. Therefore, TLADS scheme can construct routes with highly trusted nodes to the cloud, subject to a desired path length constraint. The simulation result shows that TLADS mechanism successfully avoids intrusions, even when a large portion of the data frames forwarded over the network.

References

1. Anasane, A. A., & Satao, R. A. (2016). A survey on various multipath routing protocols in wireless sensor networks. Procedia Computer Science, 79, 610-615.

2. Qiu, T., Liu, X., Feng, L., Zhou, Y., & Zheng, K. (2016). An efficient tree-based self-organizing protocol for internet of things. *Ieee Access*, *4*, 3535-3546.

3. Li, X., Zhou, C., Tian, Y. C., Xiong, N., & Qin, Y. (2017). Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. IEEE Transactions on Industrial Informatics, 14(2), 608-618.

4. Qiu, T., Lv, Y., Xia, F., Chen, N., Wan, J., & Tolba, A. (2016). ERGID: An efficient routing protocol for emergency response Internet of Things. *Journal of Network and Computer Applications*, *72*, 104-112.

5. Li, J., Hu, H., Ke, Q., & Xiong, N. (2017). A novel topology link-controlling approach for active defense of nodes in networks. *Sensors*, *17*(3), 553.

6. Tang, J., Liu, A., Zhang, J., Xiong, N. N., Zeng, Z., & Wang, T. (2018). A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks. *Sensors*, *18*(3), 751.

7. Lee, S. K., Bae, M., & Kim, H. (2017). Future of IoT networks: A survey. *Applied Sciences*, *7*(10), 1072.

8. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975.

9. Reddy, V. B., Negi, A., & Venkataraman, S. (2018, October). Trust computation model using hysteresis curve for wireless sensor networks. In *2018 IEEE SENSORS* (pp. 1-4). IEEE.

10. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network. *IEEE Sensors Journal*, *15*(12), 6962-6972.

11. Wu, X., Huang, J., Ling, J., & Shu, L. (2019). BLTM: beta and LQI based trust model for wireless sensor networks. *IEEE Access*, *7*, 43679-43690.

12. Ye, Z., Wen, T., Liu, Z., Song, X., & Fu, C. (2017). An efficient dynamic trust evaluation model for wireless sensor networks. *Journal of Sensors*, *2017*.

13. Zhao, J., Huang, J., & Xiong, N. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. IEEE Access, 7, 33859-33869.

14. Singh, S., & Sidhu, J. (2017). Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers. Future Generation Computer Systems, 67, 109-132.

15. Somu, N., MR, G. R., Kirthivasan, K., & VS, S. S. (2018). A trust centric optimal service ranking approach for cloud service selection. Future Generation Computer Systems, 86, 234-252.

16. Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D. (2019). Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. IEEE Access, 7, 9368-9383.

17. Siadat, S., Rahmani, A. M., & Navid, H. (2017). Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model. *The Journal of Supercomputing*, *73*(6), 2682-2704.

18. Huang, Longtao, Shuiguang Deng, Ying Li, Jian Wu, Jianwei Yin, and Gexin Li. "A trust evaluation mechanism for collaboration of data-intensive services in cloud." Applied Mathematics & Information Sciences 7, no. 1L (2013): 121-129.