Trust Establishment For Detecting Aggressor Nodes And Improving Route Stability In Wsn-Iot

[1]L. Sasirega, [2]Dr. C. Shanthi

[1]Research Scholar, Department of Computer Science VISTAS, Chennai, Tamil Nadu, India.
E-mail: lsasirega1975@gmail.com
[2]Assistant Professor, Department of Computer Science VISTAS, Chennai, Tamil Nadu, India.
E-mail: shanc08071978@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: In Wireless Sensor Network (WSN) constructing a secure routing between nodes is a difficult task. Removing the aggressor nodes highly improves the network performance and therefore an Efficient Routing through Node Stability Trust Evaluation is proposed here. Here the trusted nodes are detected through their node stability function with their hybrid trust values that includes direct trust and recommended trust values. Once the trusted nodes are identified then the route stability function is applied to detect the reliable routes. Route stability functions calls the route maintenance whenever the transmission requires re-routing. To reduce the re-routing process the reliable routes are detected by selecting link stability and trusted energy efficient nodes before transmitting the data. Simulation analysis is carried out and the comparisons are done with the conventional protocols.

Keywords: Aggressor nodes, Direct trust, Recommended trust, node stability, route stability.

1. Introduction

WSN is deployed with large number of tiny sensor nodes and each node is connected with each other so that it can also act as a router. The links exists between them are temporary and the nodes are having the capability of sensing and transmitting the sensed information from one end to the other or directly from source to the Base Station (BS). Recently WSN is widely applied in several applications such as surveillance, health care communication and disaster management system, etc [1]. In contrast with other existing wireless networks [2] a lot of limitations were obligated on tiny sensing nodes [3] based on their characteristics like energy resources, power and memory constraints and storage capabilities. The main goal of WSN is to place the sensor nodes in the frequently unattend-able areas to provide the uninterrupted connectivity through remote structure. Distance based clustering algorithms [4] and various routing protocols are developed for upgrading the performance better as well as to develop the network environment.

Internet of Things (IoT) seems to be a complex as well as dynamic in an unpredictable wireless atmosphere, and the existing protocols will not be a suitable one for the IoT applications [5]. Larger data generation causes network threats in some events due to the fast growth in IoT systems, that may spoils the growth of IoT [6]. The sensor nodes are easily exposed to several security attacks wile it operates individually although many protocols in related to secure and reliable routing were proposed [7] that requires cryptographic and encryption mechanisms in order to protect it leads to high processing capability and routing cost. Therefore to avoid high computational cost and tp remove malicious node, the evaluation of trust among the nodes is essential so that the sensed information can be forwarded without any modifications or distortions [8].

2. Related Works

Several trust based routing algorithms were proposed and some of the protocols are discussed here. Nodes are exposed to unpredictable behaviours because of intruders, security attacks, false report generation etc. many routing protocols is designed with security factors in its forwarder selection. Security factors and trust based routing both are to be considered during forwarding the data in the network [9, 10]. However considering both factors are still very limited.

Trust and Energy aware Routing Protocol (TERP) [11] was proposed for WSNs that comprises energy metric, trust factor and hop-count for designing the routing mechanism. Packet_forwarding behaviour is monitored for each of the nodes i.e. for single-hop communication also through licentious learning. Therefore the total trust is computed by taking the weighted sum of direct trust, oblique trust and expected probability of positive behaviours. Hierarchical Trust-based Model (HTM) is considered for evaluation of node trusthworthiness using Analytical Hierarchical Process (AHP) [12]. Later the HTM is embedded with the distributed trust-based protocol called Adaptive Trust-based Routing Protocol (ATRP). The reputation is measured by taking its previous interactions and its behaviours which is obtained through Q-learning.

Trust-aware Routing Protocol with Multi-attributes (TRPM) was proposed here a cluster structure is taken to divide the nodes into group or clusters on the basis of adjacent node relationship and distance during the environmental setup [13]. TRPM considers direct trust (feedback ratings and packet forwarding), data trust (accuracy) metrics, energy trust metric (energy level variations), and recommendation trust (recommendation response request) as evaluation metric [14]. The indirect trust is computed through recommendation comparison from neighbours (their own trust rate). More number of nodes may be connected with the elevator because of uneven number of deployment of nodes.

Each trust agent in the ATRP starts without any previous interaction experience initially and the evidence of direct trust agent gradually overfills the time [15]. The confidence level here is denoted as 'γ' and it is used to represent interaction weights, if interaction count with trustee increase, then 'γ' value also increases. With respect to the elapse time the value of the trust also decreases and hence the tracking of relevant trust value is mandate. ATRP is carried out with some exponential decay time factor [16] that is utilised for updating the trust value. The exponential decay time factor is utilised in the ATRP protocol and if the γ value of is lesser than 1, then consequence of recent interactions are much significant than the older interactions.

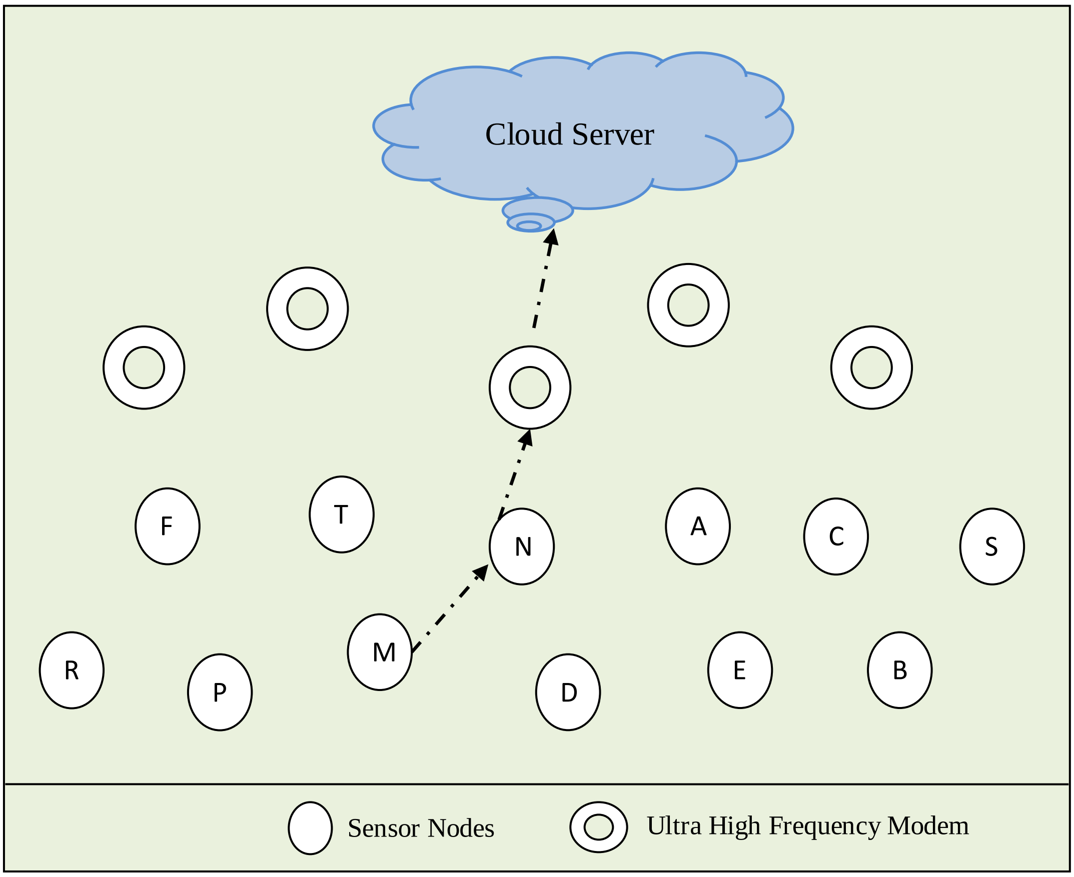
Node level trust is determined using the proposed methodology called Node Level Trust Evaluation (NLTE) protocol [17]. The node trustworthiness is measured by using the internal resource of the node. The topology of the network is independent and it is a fully mediating process with second-hand data. Node response evaluates the trust value on its own along with the interactions considered such as self-scrutiny and self-attestation algorithms. Energy-aware and Secure Multi-hop Routing (ESMR) protocol [18] was proposed. Secret sharing scheme was used to improve network performance in terms of energy efficiency and security over malevolent actions. Three aspects are considered here, first, the network is splitted into inner and outer zones, second the nodes are grouped into clusters on basis of neighbourhood vicinity and secure the data using secret sharing method and at last the quantitative analysis is done to reduce the routing failures.

Several trust models are carried out and represented in [19] with respect to the security needs of the IoT system, such as SecTrust RPL [20], DCTM-IoT, CTRUST, etc. Here security issues and IoT system requirements as well as Routing Protocol and Lossy networks (RPL) protocol are all described along with the various attacks, includes man-in-the-middle attack, sppofing, black-hole, ranking, etc. in addition, different mitigation schemes and the importance of trust models in IoT for the purpose of resultant secure routing are also analyzed.

3. Proposed Method

The protocol named Efficient Routing through Node Stability Trust Evaluation (ERNSTE) is proposed. Here the trusted nodes are detected through their node stability function with their hybrid trust values that includes direct and recommended trust values. Once the trusted nodes are identified then the route stability function is applied to detect the reliable routes. Route maintenance is required whenever the transmitted data fails in the middle or any route failure occurs. Route maintenance is required whenever the transmitted data fails in the middle or any route failure occurs. Hence route stability function is applied in order to reduce the re-routing process the reliable routes are detected by selecting link stability and trusted energy efficient nodes before transmitting the data. Figure 1 shows the example scenario of cloud assisted ERNSTE framework.

Figure 1: Network Scenario of ERNSTE



(i) Node stability function

The node stability function is carried out in preliminary stage once the nodes are deployed in the environment. The node undergoes the hybrid trust evaluation and it includes direct trust and the probability of recommendation trust. It is computed through the weight of the node's interaction. If the weight of the interactions is less, then the node is tagged as aggressor nodes. Probability of recommendation trust measures the node accuracies using the computed node interaction values presented towards the neighbour of source nodes.

a. Direct Trust: Packet forwarder mechanism is applied to compute the node's direct trust value initially. The node 'M' forwards the packet to 'N' with node trust value 't1' and node 'N' forwards the packet to 'X' is t2 which is shown in figure 2, consequently the node evaluates the trust accuracy of obtained t1 and t2; each node holds the trust probability value of (0, 1) if t1 = t2 then the nodes are trustable with the value 'DT(1)'. Once the DT(A) of node 'A' is computed and holds the DT value has DT(1) then the node 'A' is listed in trustable nodes and if the DT value not matches i.e. t1!=t2 then the node 'A' holds the trustable value of '0' i.e. DT(0). Computation of direct trust accuracies for nodes is obtained using equation 1.

$$DT(\mathrm{X})_{\mathrm{M,N}} = \frac{M\_Data\ fwd' \rightarrow N}{N_{data} + Pkts\ drops' \rightarrow X} \qquad (1)$$

```
Direct Trust Computation Algorithm
Begin
Proc (Direct Trust 'DT')
Data forwards from 'M' to 'N' → DF(Pn)
Data forwards from 'N' to 'X' → DF(Pn+1)
Compute DT for DF(Pn) → DT(t1)
Compute DT for DF(Pn+1) → DT(t2)
If $DT(X_{(M,N)})$ → DT(t1)≡DT(t2)
$DT(X_{(M,N)})$ holds DT(1)
Listed in trustable nodes
Else
$DT(X_{(M,N)})$ holds DT(0)
```

```
Falls under aggressor node list
End
```

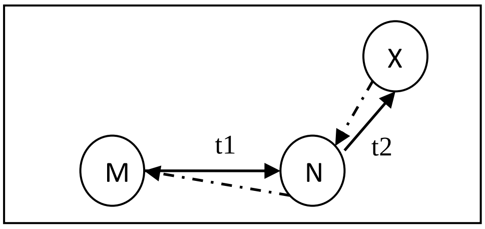


Figure 2: Direct_Trust

b. Recommended Trust (RT): The accuracy of recommended trust is computed by using weighted Dempster-Shafer trust ratio between the nodes. The probability of recommendation trust is computed among the source node and its neighbour nodes, let assume the nodes ‘M’ and ‘N’ are neighbour nodes and it is represented as Y_{MN} then the probability of recommended trust for node ‘N’ is computed at node ‘M’ using the equation 2.

$$RT_{M}^{N}(t)=\sqrt{\frac{(\sum_{y\in Yab} DT_{M}^{Y}(\mathrm{t})-DT_{N}^{Y}(\mathrm{t}))^{2}}{\left|Y_{MN}\right|}} \tag{2}$$

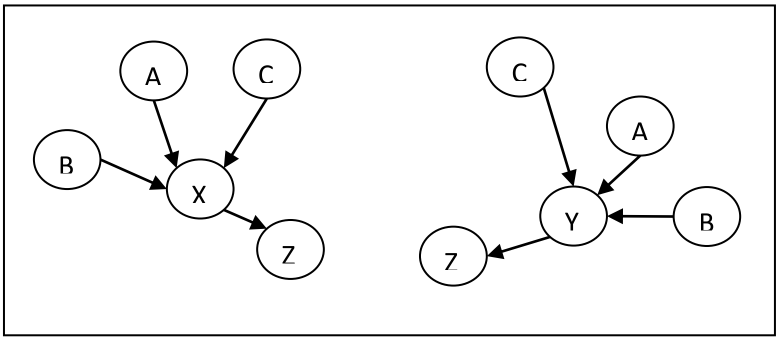


Figure 3: Recommendation trust for ‘Z’

Table 1: RT values for node ‘Z’ headed from ‘X’

Node	RT
A	0.91
B	0.88
C	0.85
X	0.90

Using the node’s direct trust values the recommended trust ratio for the other nodes that is located in the communication range of source node. Therefore the recommended trust value for each node is obtained by fusing the direct trust values with the current trust values. Here, X denotes direct trust values obtained for the neighbour nodes and Y represents the recommended trust given for the neighbour nodes, therefore RT is obtained using equation 3.

$$R_{M}^{N}(T)=(1-\mathrm{D}_{M}^{N}(\mathrm{t}))\times\frac{\sum_{i\in X_{MN}}(\mathrm{Xi}\wedge\mathrm{Yi})}{Ni} \tag{3}$$

Table 2: RT values for node ‘Z’ headed from ‘Y’

Node	RT
A	0.84
B	0.89
C	0.92
Y	0.93

Here n denotes the sum of number of recommendation trust values. Figure 3 represents the model recommendation trust value of node ‘Z’ with respect to their neighbour nodes ‘X’ and ‘Y’. Therefore the recommendation trust for the node ‘Z’ can be obtained by fusing the trust values of node ‘A’ ‘B’ and ‘C’ obtained through ‘X’ and ‘Y’. Table 1 consists of the assumed RT values of nodes headed from ‘X’ and table 2 represents assumed RT values of nodes headed from ‘Y’

Table 3: Resultant Nodes

DT	RT	Resultant Value
0	0	TN
0	1	AN
1	0	AN
1	1	TN

Finally the node stability function is evaluated through the trust values obtained through the both DT and RT. If both DT and RT of the nodes are found to be same then the particular node is added in the Trustee Node (TN) list. If the resultant node trustee value seems to be different then it is marked as Aggressor Node (AN) and removed from the routing table. Table 3 gives the resultant trusted node obtained through DT and RT values.

Algorithm for Recommendation Trust Evaluation

```
Proc (Recommended Trust (Ni))
DT(M) & DT(N) arrays listed for nn of ‘M’ & ‘N’
Direct_Trust ← 0
Recommended_Trust_count ← 0
For Ni ← 0 to |Ni_MN|
Direct_Trust ← $\sum D\_T_{MN} + [(D\_T(M)) - (D\_T(N))]^2$
If [(Direct_Trust(M))  – (Direct_Trust(N))] < δi
Then Recommended_Trust_count ← R_T_count+1
Do $DT(M,N) = \frac{\sqrt{D_T/|Ni_{MN}|)}}{nn}$
Prob(RT)$_{M,N}$ ← (1-D$_{(M, N)}$) x (Recommended_Trust_count)/|N$_{MN}$|
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 chosen for transmitting the data to the cloud server.

(ii) Route Stability Function

The data from the sensor nodes are transferred to the cloud server by choosing the trusted nodes. However the aggressor nodes are removed from the routing by selecting the trusted nodes however the resource management should be followed for protecting the network lifetime. The route maintenance component is carried out for minimizing the damages of routes in the middle of transmission process and data re-forwarding. If the protocol thinks that the selected route is not suitable for further transmission process due to the loss of link connectivity between the trusted nodes or energy degradation factor or some other routing issues occurred. Then the discovery of alternative routing path for data transmission from the sane sender node should be selected. Mainly, in the term of the succeeding condition the route maintenance process is called over.

The link connectivity between the nodes is tested and the nodes has high communication ratio or the nodes falls under the same communication range with less transmission time are selected for the data transmission process. The link connectivity threshold is set with respect to the received signal strength at some boundary instant. This is updated in the route maintenance process.

Secondly, the energy level that is currently remained in all the trusted nodes are evaluated in order to transmit the data reliably. Since the low energy nodes that present in the routes might act as selfish nodes which leads to data loss and causes performance degradation and the entire network gets collapsed. Therefore the energy level should be maintained for all the nodes and the higher energy level should be selected for the routing process. Therefore the trusted reliable route RR_T can be estimated using equation 4.

$$RR_T = \sum_{i=0}^{n} LC_{(\mathrm{Ni})} + EL_{(\mathrm{Ni})} \quad (4)$$

Therefore the reliable and trusted routes are selected for the data transmission process from the sensor nodes to the particular cloud server. Thereby the user or clients can access the trusted and reliable data.

4. Analysis of Simulation Results

Simulation analysis is done with the simulation tool called Network Simulator (NS) of version 2.35, here the network performance and the system efficiency for both conventional and proposed mechanism. The events are analysed discreetly in a network scenario. The parameters that are taken for the analysis are delivery rates of packets, energy consumption, False Node detection ratio, average delay and Node trust ratio.

Table 4: Simulation Metrics

Parameter's	Value
Channel Type	Wireless channel
MAC	IEEE 802.11
Simulation Area	1000 x 1000m, 800 x 800m
Protocols	ERNSTE, NLTE & ESMR
Transmission range	250mts
Antenna Type	Omni antenna
Node Density	100
Network Interface Type	WirelessPhy
Data_rate	11Mbps

The proposed scheme is represented as ERNSTE and the conventional schemes taken for the comparison are NLTE and ESMR. The remaining parameters that are considered in the network animator window for the analysis of simulation results for both proposed and conventional protocols are given in the table 4.

(a) Delivery Rates of Packet

Delivery Rates of Packets (DR_P) can be defined as the rate of packet traffic that is passed over the data channel to the cloud surface or receiver end with respect to the considerable amount of sent packets from the sender node. DR_P is calculated using equation 5.

$$DR_p = \frac{\sum Rate\_Pkts\,dlvrd}{\sum Rate\_Pkts\,sent} \quad (5)$$

Figure 4 shows the graphical representation of proposed ERNSTE scheme and conventional protocols such as NLTE and ESMR. It is clear that the proposed scheme has better delivery rates at the receiver end comparing to their conventional schemes. Increasing the density of nodes is directly proportional to the rate of delivery of data packets. Therefore this metric DR_P is proved for its better efficiency of the proposed technique.

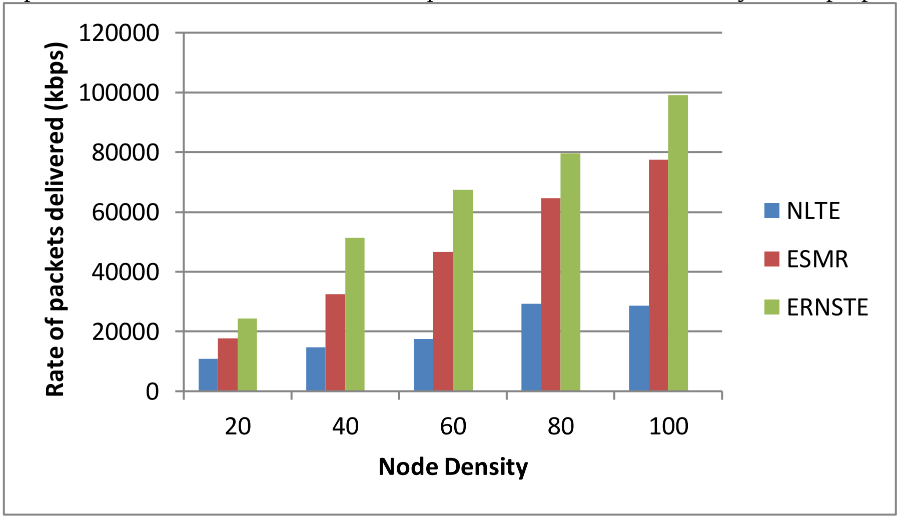


Figure 4: Delivery Rates of Packets

(b) Energy Consumption

The level of energy per node that is consumed during the data processing and transmission is said to be energy consumption of that particular node at some instant of time. Energy consumption calculation is computed for the detection of remaining energy level that is left in each node present in the network.

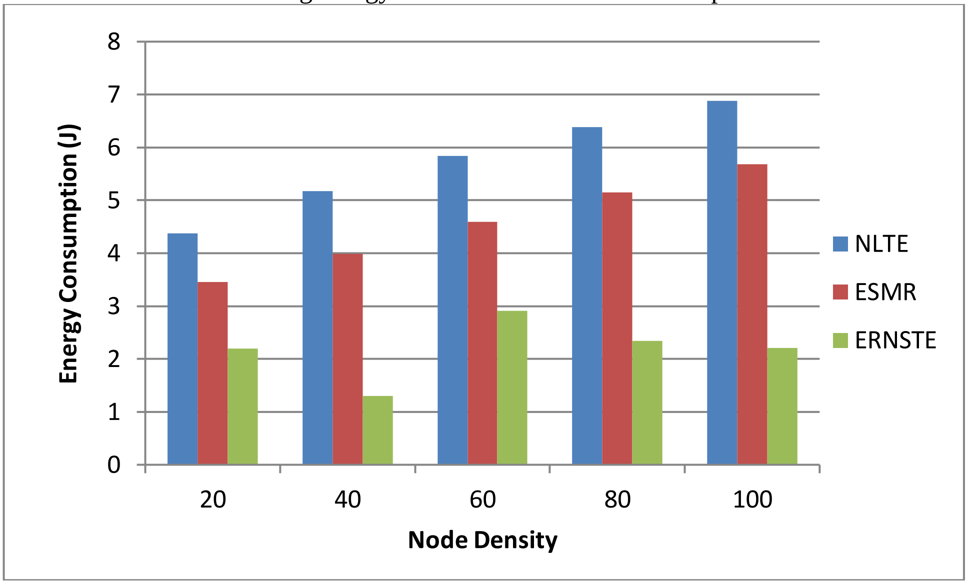


Figure 5: Energy Consumption

The graphical representations of energy consumption for both the proposed and conventional schemes are represented in figure 5. The energy that is consumed by the nodes for the proposed scheme is low compared to the existing schemes NLTE and ESMR. Thereby this proves that the selected routes are more reliable and resource constraint.

(c) End to End Delay

End to End (ETE) delay is calculated by taking the time difference that exists during the transmission time of sent packets and the time of packets receiving at the receiver end. ETE delay is calculated for all set of data transmissions that takes place in the network which is measured using the equation 6. Here n denotes the node density.

$$ETE\_Dly = \frac{\sum_0^n (PktRcvd\_Time - PktSent\_Time)}{n} \tag{6}$$

The time difference that is obtained for both the proposed ERNSTE scheme and the conventional NLTE and ESMR schemes is shown in the figure 6. Proposed method ERNSTE exhibits lower delay values for sending and receiving packets in terms of processing ETE delays. Hence it is proved to be the ERNSTE protocol consumes minimum time for the execution process that includes processing, transmission and reception of packets compared to existing protocols.

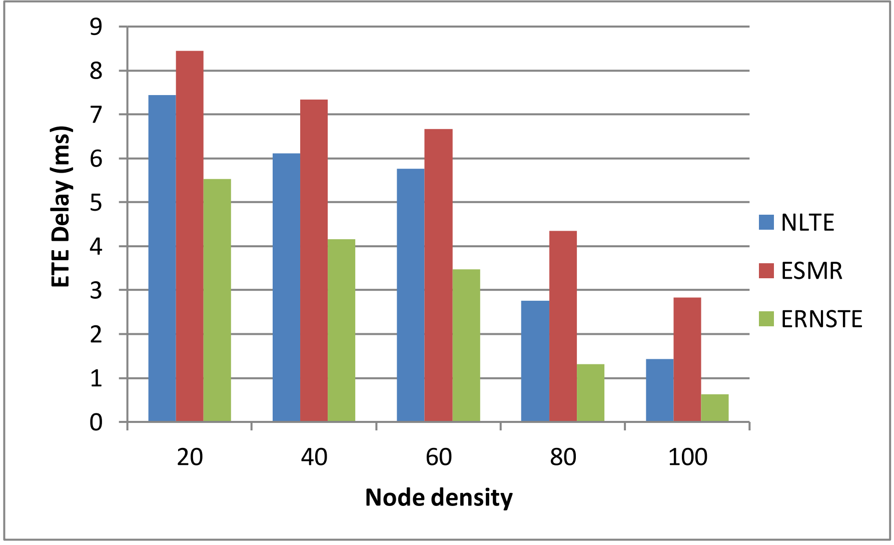


Figure 6: ETE Delay

(d) False Node Detection Ratio

The ratio between the number of trustable (normal) nodes and the number of aggressor (malicious) nodes is measured and it is defined as False Node Detection Ratio (FNDR). FNDR is determined through the node's packet forwarding behaviour i.e. the total number of packets that successfully delivered over the channel with respect to their sent packets successfully.

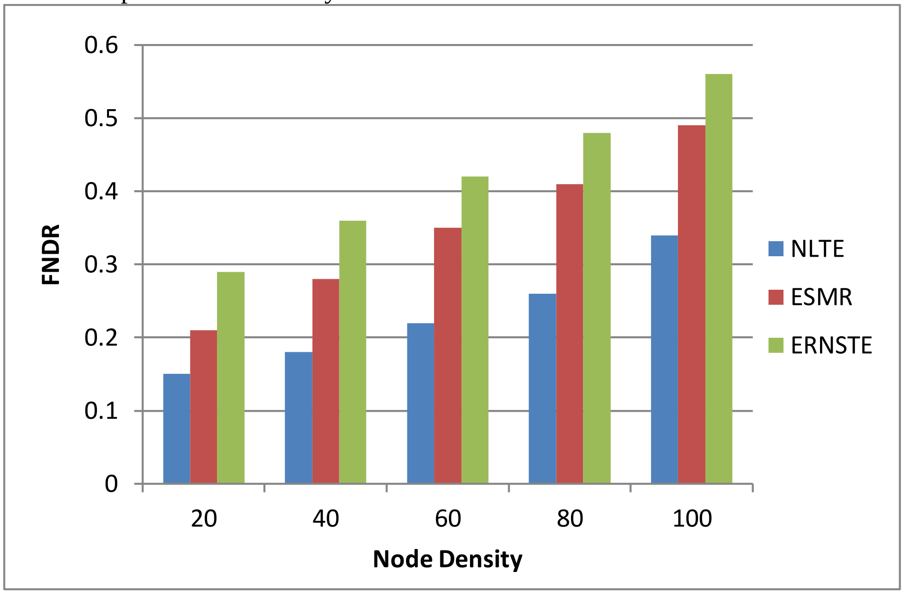


Figure 7: FNDR

FNDR for the protocols ERNSTE, NLTE and ESMR is shown in figure 7 as geographical representation. 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.

(e) Node Trust Ratio

Node Trust Ratio (NTR) is defined to be the ratio of trust values obtained for the nodes with respect to their context packet forwarding behaviour. Ratio of trustable nodes that are selected for the data transmission is based on measuring the node's trust value. NTR is determined in regards of number of nodes that present in the network.

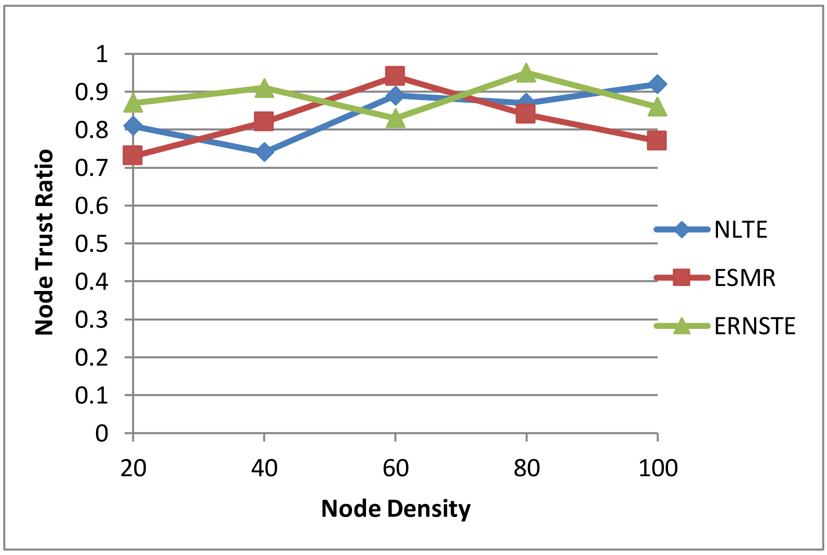


Figure 8: Node Trust Ratio

Figure 8 gives the graphical representation of NTR with respect to the node density for the proposed ERNSTE and the existing schemes such as NLTE and ESMR. The average NTR is calculated for the proposed ERNSTE protocol is 0.88 and for existing protocols such as NLTE and ESMR, the obtained average NTR values are 0.84 and 0.82 respectively. Therefore it is proved that the proposed scheme selects better trustable nodes for routing the data without major loss.

5. Conclusion

Efficient Routing through Node Stability Trust Evaluation is proposed here. Here the trusted nodes are detected through their node stability function with their hybrid trust values that includes direct and recommended trust values. The trusted nodes are identified then the route stability function is applied to detect the reliable routes. Route stability functions calls the route maintenance whenever the transmission requires re-routing. To reduce the re-routing process the reliable routes are detected by selecting link stability and trusted energy efficient nodes before transmitting the data. Simulation analysis is carried out and the comparisons are shown in the result section along with the conventional protocols.

References

1. Eddine-Boubiche, D., Trejo-Sánchez, J. A., Toral-Cruz, H., López-Martínez, J. L., & Hidoussi, F. (2018). Wireless sensor technology for intelligent data sensing: Research trends and challenges. In Intelligent data sensing and processing for health and well-being applications (pp. 41-58). Academic Press.
2. Meng, T., Wu, F., Yang, Z., Chen, G., & Vasilakos, A. V. (2015). Spatial reusability-aware routing in multi-hop wireless networks. IEEE Transactions on Computers, 65(1), 244-255.
3. Rani, S., Talwar, R., Malhotra, J., Ahmed, S. H., Sarkar, M., & Song, H. (2015). A novel scheme for an energy efficient Internet of Things based on wireless sensor networks. Sensors, 15(11), 28603-28626.
4. Ruan, F., Yin, C., Chen, J., Wang, J., & Xue, S. (2013). A distance clustering routing algorithm considering energy for wireless sensor networks. International Journal of Future Generation Communication and Networking, 6(5), 73-80.
5. Lazarescu, M. T. (2013). Design of a WSN platform for long-term environmental monitoring for IoT applications. IEEE Journal on emerging and selected topics in circuits and systems, 3(1), 45-54.
6. Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. Ad Hoc Networks, 32, 17-31.
7. Krishna, M. B., & Doja, M. N. (2015). Multi-objective meta-heuristic approach for energy-efficient secure data aggregation in wireless sensor networks. Wireless Personal Communications, 81(1), 1-16.
8. R. K. Kodali and S. Soratkal, "Trust model for WSN," 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, 2015, pp. 903-906, doi: 10.1109/ICATCCT.2015.7457012.
9. Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2014). An efficient distributed trust model for wireless sensor networks. IEEE transactions on parallel and distributed systems, 26(5), 1228-1237.
10. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.
11. 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.
12. Khalid, N. A. (2019). Distributed trust-based routing decision making for WSN (Doctoral dissertation, Auckland University of Technology).
13. Sun, B., & Li, D. (2017). A comprehensive trust-aware routing protocol with multi-attributes for WSNs. IEEE Access, 6, 4725-4741.
14. Khan, W. Z., Saad, N. M., & Aalsalem, M. Y. (2012, June). An overview of evaluation metrics for routing protocols in wireless sensor networks. In 2012 4th International Conference on Intelligent and Advanced Systems (ICIAS2012) (Vol. 2, pp. 588-593). IEEE.
15. Yu, H., Shen, Z., Leung, C., Miao, C., & Lesser, V. R. (2013). A survey of multi-agent trust management systems. IEEE Access, 1, 35-50.
16. Duan, J., Yang, D., Zhang, S., Zhao, J., & Gidlund, M. (2013, November). A trust management scheme for industrial wireless sensor networks. In IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society (pp. 5576-5581). IEEE.
17. Desai, S. S., & Nene, M. J. (2019). Node-level trust evaluation in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 14(8), 2139-2152.
18. Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., & Guizani, N. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. IEEE Access, 7, 79980-79988.
19. S. M. Muzammal, R. K. Murugesan and N. Z. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4186-4210, 15 March15, 2021, doi: 10.1109/JIOT.2020.3031162.
20. Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 93, 860-876.