INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Performance and evaluation of location energy aware trusted distance source routing protocol for secure routing in WSNs

M Rajasekaran[1]*, **A Ayyasamy**[2], **R Jebakumar**[3]

1 Research Scholar, Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamilnadu, India. Tel.: 9789165661

2 Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamilnadu, India

3 Department of Computer Science and Engineering, Faculty of Engineering and Technology, SRMIST, Kattankulathur, Tamilnadu, India

OPEN ACCESS

Received: 26.08.2020

Accepted: 25.10.2020

Published: 06.11.2020

Editor: Dr. Natarajan Gajendran

Citation: Rajasekaran M, Ayyasamy A, Jebakumar R (2020) Performance and evaluation of location energy aware trusted distance source routing protocol for secure routing in WSNs. Indian Journal of Science and Technology 13(39): 4092-4108. https://doi.org/10.17485/IJST/v13i39.1522

* **Corresponding author**.

Tel: 9789165661
smrajamani1981@gmail.com

Funding: None

Competing Interests: None

Copyright: © 2020 Rajasekaran et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To propose a suitable algorithm for improving the network lifetime of Wireless Sensor Networks (WSNs). **Methods/Findings**: We proposed a suitable Location and Energy Aware Trusted Distance Source Routing (LEATDSR) algorithm. Here, the energy consumption, location and the data quality are equalized by the Quality of Service (QoS) based routing algorithms. In addition to this algorithm, an existing clustering algorithm is also incorporates for grouping the sensor nodes based on the trust, location, energy and distance. In this LEATDSR is capable of deciding the evaluation metrics which express the QoS. Moreover, a new trust mechanism is also introduced in this model that incorporates multi-attributes of various sensor nodes in terms of communication, data, energy, and recommendation. This new trust mechanism relies on an enhanced sliding window time by considering the occurrences of attack frequency for facilitating the discovery of anomalous behaviours of attackers. The enhanced energy utilization is established within the sensor nodes for performing the active data transmission. The performance of the proposed model is evaluated by conducting various experiments in a simulation environment which creates by using NS2. From the experiments conducted in this work, the average packet transfer rate is increased drastically when compared to existing models available in the literature.

Keywords: Sensor nodes; energy; quality of service; wireless sensor network; clustering; trust

1 Introduction

Wireless Sensor Network (WSN) is becoming a part of next generation application and are widely used in various important departments like industry, weather monitoring system, army, medical and many other social domains due to drastic improvement of communication technology especially wireless communication(1). In WSNs, the transmission capacity of sensor nodes is limited based on the availability of the energy and communication range between the source and destination nodes. The attackers are always aiming to disturb the normal functionality of the sensor nodes in WSNs. For avoiding these malicious nodes activity, many techniques were proposed by various researchers using intrusion detection system, authentication and cryptography(2) for enhancing the network security. Even though, these standard security mechanisms are not enough to handle the malicious nodes.

For protecting the WSNs from attacks and distinguish trustable nodes from compromised ones, researchers introduced trust mechanisms into WSNs. Trust based routing algorithms are proposed and implemented in electronic commerce applications for identifying the legitimate users. These legitimate users are more efficient in terms of detecting the compromised nodes in WSNs. This is because the evaluation of sensor node trust value is related to the past behaviours and activities of suspicious node and also the recommendation data from trustworthy neighbour ones. According to the trust score and the rational strategies only are proposed for enhancing the security in WSNs. The major consideration while the designing a phase which are related strategies is how to select the optimal nodes that are intermediate of the secure routing process in light of trust score values. In addition, trust mechanisms with the additional such as energy cost, distance between the neighbouring nodes and the destination node or number of hops into secure routing evaluation for getting routes with better Quality of Service (QoS).

Energy is playing major role in wireless sensor networks than the other parts of wireless sensor networks such as a sensing unit that is used to monitor the network environment, a processing unit which is used to process the data, radio transceiver unit that is used for wireless communication and the power supply unit. The sensor nodes are energy constrained that relies on batteries as energy source. The wireless sensor network life time is limited when it is compared to the wired and wireless networks due to the energy constraints. In this scenario, it is difficult to reach every sensor node and replace the battery in this wireless sensor network based applications. Therefore, to reduce the energy consumption is very important which is useful for prolonging the network lifetime. Moreover, the equal energy distribution process is called energy mapping in wireless sensor networks(3). The available amount of energy in the sensor network can be used to redeploy the nodes before gets disconnected due to the energy depletion. For this purpose, routing protocols are uses the information about the energy map which is useful to reroute the data packets through eligible nodes which has high residual energy. The remaining nodes with less energy can be preserved their energy for their future usage. This all information also can be used as input values for evaluating the protocols in terms of their energy consumption behaviour in the WSNs.

Recently, trust management system which is a system that is also widely used in many applications including data aggregation, data packet routing in networks, access control mechanisms in the process of data access, and the decision-making process in intrusion detection systems(4). The term Trust Management System (TMS) is also utilized together with the processes of trust score calculation and the reputation score calculation. These two processes are important and also playing crucial roles in trust management systems. In(4), the author addresses the various trust management systems in their paper and also discusses the trustworthiness between the nodes in the networks based on the constraints like data gathering, to make effective decisions that are related to the trust computation, evaluation of the options that are related to the trust score relevancy, and the monitoring and re-evaluation of the existing trust score relevancies. In this scenario, the trust management is monitoring the behaviour of neighbour nodes while data transmissions and detecting misbehaved nodes, estimating the trust scores that are based on the detection results, and the propagation of trust score.

Moreover, the trust score threshold setting for making decision over any kind of application which is an important factor in the process of attack identification and detection. The trust threshold is used to differentiate between the malicious node and the benevolent node. The trust threshold is chosen in most of researchers according to the previous literature only(5–7). They fixed as a trust threshold between 0.5 and 0.9. In addition, majority people used the mean value of trust score as a trust threshold. Later, routing process can be secured by considering the trust scores for making final decisions over the nodes whether those nodes can be participated in the routing process or not. Route can be finalized according to the trust score of the node and the average trust score of the established routing path.

In this study, a new routing algorithm called Location and Energy Aware Trusted Distance Source Routing (LEATDSR) algorithm is proposed to improve the network lifetime and the QoS of WSNs. Here, the energy level of participating nodes are measured and monitored for confirming the participation in a cluster according to the current location of the node. Moreover, the different types of trust scores such as data quality trust score, data communication trust score, energy trust and the overall trust which are able to detect the various attacks like black-hole attacks and grey-hole attacks before the routing process for enhancing the QoS. In addition, an existing clustering algorithm called K-Means clustering algorithm is also incorporates for grouping the sensor nodes based on the trust, location, energy and distance in this work. In this LEATDSR is capable of deciding the evaluation metrics which express the quality of service.

Rest of this paper is organized as follows: Section 2 provides the literature survey in this direction. Section 3 explains the system architecture. Section 4 described the proposed work in detail. Section 5 shows the experimental results and discussion. Section 6 gives conclusions and also suggests some future directions.

2 Literature Survey

There are many works have been done by various researchers in the direction of Routing, Clustering, Secure routing, Trust based routing, energy aware routing[8] and location aware routing techniques in the past. Among them,[9] a new and energy efficient clustering protocol called Prolong Stable Election Protocol for improving the network lifetime was proposed. They have selected the cluster head randomly in each iteration for balancing the load, consume less energy and also to enhance the network lifetime. In[10], a fuzzy logic based routing technique which is used to make effective decision based on the different parameters such as energy consumed by the nodes, mean value for the distance between two nodes, number of adjacent nodes and average distance between the adjacent nodes and the destination node in the network. They have considered an energy level as a threshold for intra-cluster routings and the inter-cluster routings through multi-hop communication method in order to reduce the energy consumption. They achieved better performance in terms of energy consumption and the network lifetime.

In[11], an energy-efficient and cluster based routing algorithm for framing a balanced clusters and also for enhancing the network lifetime by using cluster heads in WSNs was designed. Moreover, they also used the existing fuzzy c-means clustering algorithm for forming a cluster and used the Sugeno fuzzy modelling for identifying the suitable cluster head for further process in their routing technique. In[12], a new clustering algorithm called multi-clustering algorithm. In their algorithm, cluster the sensor nodes that are grouped by using various clustering algorithms. In addition, they are not selecting the cluster heads in each round for reducing the number of transmission messages.

In[13], a new trust mechanism was designed; which is able to identify the trust worthiness node which able to behave as a black-hole attack and grey-hole attack. In[14], a new trust based energy-efficient secure routing algorithm was developed, which works based on active trust that performed well over the black-hole attacker detection. They also proved that their model able to reduce the energy consumption and to improve the network lifetime. Moreover, their model considered only how to resist the black-hole attack while trust assessment process that makes it no security against other attacks.

In[15] an ambient trust based sensor routing was introduced, which combines with the existing geographical routing methods. Even though, the routing protocol is contributed for considering the multiple factors such as energy and data into the trust score evaluation between the nodes. The authors claimed that their model achieved better performance in terms of packet delivery ratio and the network lifetime than the other existing models. In[16], a new algorithm called trust prediction and trust-based source routing algorithm was proposed. In their routing algorithm, each node achieves packet delivery accuracy rate as evaluation criterion when it computed the trust value of neighbour node. The speciality of their routing algorithm is to avoid the recommendations from the third-party nodes in the whole trust calculation process of WSNs. In addition, the optimal path selection process is completely executed by the destination node in this proposed algorithm. Moreover, it consumed more residual energy of destination node that reduced the network lifetime.

In[17], a new Context Aware Adaptive Fuzzy (COAAF) based context aware protocol was proposed. COAAF is adaptive for variable services and network traffic intensity. In[18], an efficient and distributed trust model for restructuring the trust mechanism was proposed to consider the additional factors along with communication, data and energy simultaneously. In their model, the existing multi-hop indirect trust calculation technique that enhances the accuracy of trustworthy path selection process. In[19], a new protocol called Enhanced Interior Gateway Routing Protocol (EIGRP) was proposed for preserving the energy by reducing the network traffic in which the routing decisions were managed over the network automatically. Their protocol works according to the diffused update algorithm for finding the shortest path which is the aim of WSNs. Moreover, they used the duty cycling is commonly for preserving the energy effectively. In their scheme, the cluster heads play a major function in WSN. The major objective of their scheme is to enhance the network lifetime and also to preserve the energy.

The wireless sensor network threats have two categories, that also analyse the defensive capability of trust aware secure routing mechanisms introduced in related work against the various kinds of malicious attacks. Moreover, they also proposed a new robust and trust based routing protocol with multi-attributes in terms of energy, communication, data, and recommendation for assisting the sensor nodes which are available in establishing and reliable routes during sliding window time technique that combines with attack frequency detection mechanism that is used to identify the various attackers with mutable attack frequency. Finally, they achieved better performance for their proposed mechanism by achieving the better detection rate, high packet delivery ratio and less time taken and also increases the network lifetime. In[20], a new routing algorithm called Power-Aware Distance Source Routing (PADSR) clustering algorithm was proposed. PADSR considered the node energy level for performing effective routing. For measuring the participating nodes energy level, authors introduced a new energy model called Radio Energy Model that is incorporated with PADSR for energy efficient routing in WSNs.

In [21], a new protocol called SecTrust-RPL was proposed, which works on RPL protocol that uses a new trust mechanism for evaluating the sensor nodes to take decision over the routing process while isolating the malicious nodes in the wireless sensor networks. Their system computes the nodes trust by examining the successful data exchange between the nodes in order to determine the nodes reliability to forward the data packets to other nodes within the RPL network. Moreover, it also facilitates to detect the malicious node and isolate the procedure which is able to detect and isolate the suspicious nodes while optimizing the throughput performance. The experiments have been conducted for evaluating the performance of their system and show that the efficacy of their system.

A new routing mechanism was designed and implemented as "Energy-efficient Trust Management and Routing Mechanism" [22] for the wireless sensor networks to handle the malicious attacks namely selective forwarding attack and new-flow attack. In their mechanism, they extended the sensor flow tables for realizing a light-weight trust monitoring and the evaluation scheme at the node level.

In [23], a new routing algorithm called Energy-Efficient Grid-Based Routing algorithm for enhancing the network life time was proposed. The authors used fuzzy logic for choosing the suitable grid coordinator by considering the energy level of the sensor nodes. The energy consumption is reduced due to the use of effective fuzzy logic for decision making. The data transmission between the source and destination is performed through the grid coordinator that acts as relay node and also it reduces the energy consumption in the routing process that has enhance the network lifetime. They applied fuzzy rules for node deployment, energy analysis, cluster formation, cluster head selection process and routing through cluster heads. Finally, they enhanced the network lifetime and packet delivery ratio, and reduced the energy consumption.

Spatial and Energy enhanced trusted DSR technique for providing security and energy utilization in WSN data transmission [24]. The energy efficient Region-based technique has been implemented for providing the enhanced lifetime in WSN [25]. The reliable cluster based energy utilization and secure routing is constructed in heterogeneous WSNs [26], the reliable routing with energy enhanced data transmission in WNS [27–31]. The evolution of IoT connects the objects to the networks despite monitoring physical and environmental conditions. Several metrics are used to establish the communication for determining the energy consumption [32]. The scheduling nodes of WSN may minimize the energy consumption of the sensor nodes that the energy threshold based coverage algorithm enhances the lifetime of the network and also improves the energy consumption [33]. LEACH centralized sleeping protocol for WSN has been constructed to enhance the network lifetime according to the sensing data within the time limit. The hybrid algorithm provides the quality of service and reduced end-to-end delay compared with other LEACH protocols [34].

First, they proposed a centralized trust model at the controller level for detecting and isolating the malicious nodes that are based the trust information that are collected from various sensor nodes. Second, authors presented an energy-efficient report message aggregating scheme for selecting the aggregation points to save the energy and also ensure the transmission of control traffic. Third, they present a trust and routing mechanism together by considering the residual energy of sensor nodes and the trust level to guarantee the transmission of data traffic. They demonstrated that the proposed architecture detects and responds to the internal network attacks, such as Greyhole, Blackhole, new-flow attacks, efficiently and also enhances the performance in terms of energy consumption and network life time. A new clustering technique was also used in their work for performing effective routing process through cluster heads that helped to save the energy available in the nodes.

3 System Architecture

The overall architecture of the proposed system is shown in Figure 1. It consists of nine major components such as sensor nodes, data collection module, energy manager, temporal manager, spatial manager, decision manager, trust module, energy module and secure routing module. Sensor nodes that consist of various nodes with minimum energy level which are participated in the wireless sensor network. Data collection module is responsible for collecting the necessary details from the sensor nodes. The collected information is forwarded in to the decision manager. The decision manager is act as a coordinator for the overall architecture. It has overall control over the proposed work.

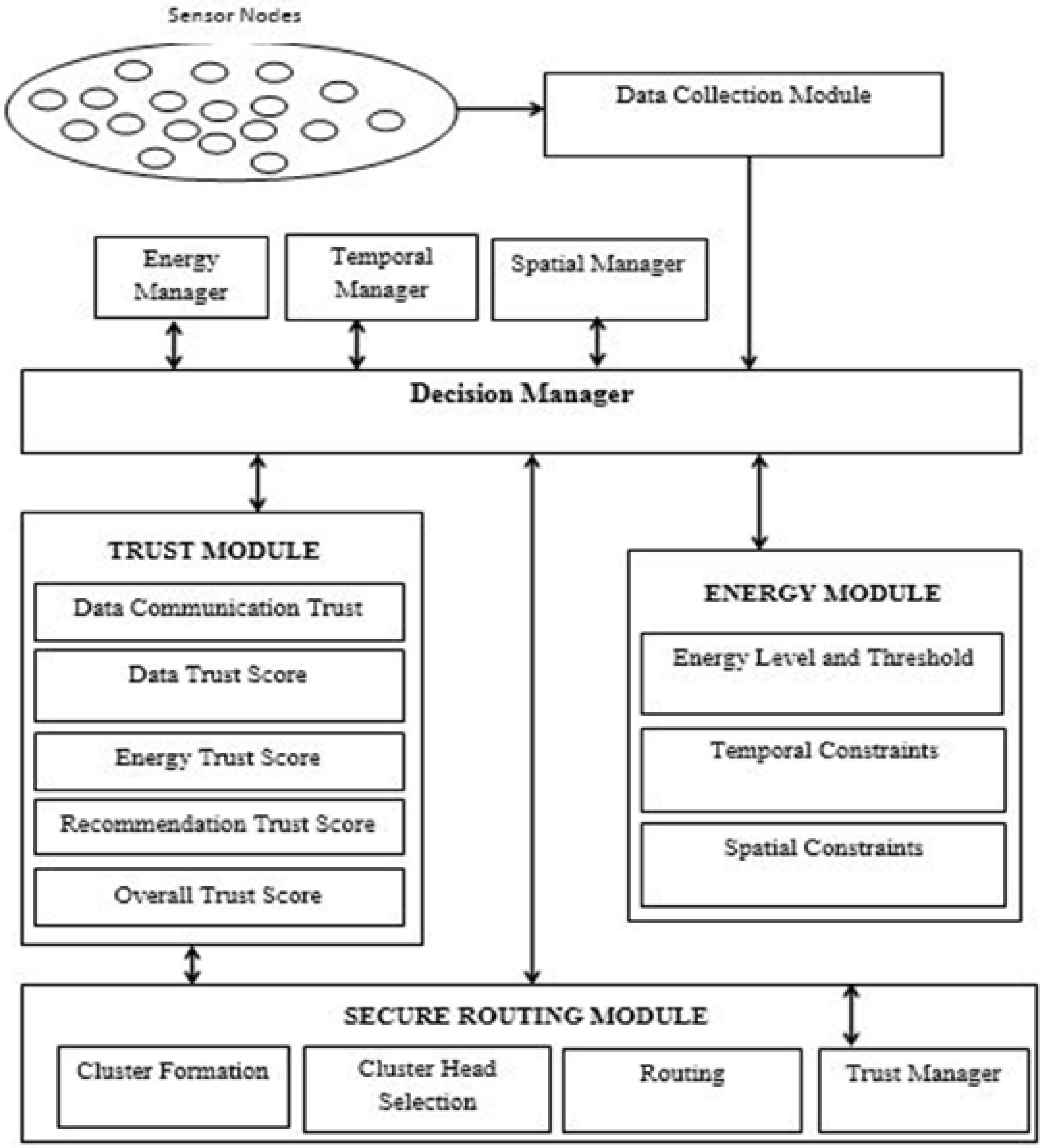

Fig 1. System architecture

The decision manger is responsible for collecting the necessary data from data collection module and it calculates the trust score based on the genuineness of the sensor nodes with the consideration of time and location of the respective sensor nodes. Moreover, it takes decision over the sensor nodes which are to be identified as energetic nodes in the network with the help of energy manager recommendation. In addition, the routing decision also finalized by this decision manager according to the energy level and the trust score of sensor nodes.

The energy module consists of three sub modules such as energy threshold, temporal constraints and spatial constraints for balancing the energy level based on the spatial and temporal constraints. The trust module consists of five sub components namely data communication trust, data trust score, energy trust score, recommendation trust and overall trust score. These five sub components are used to calculate the direct and indirect trust scores. Here, all these scores are calculated dynamically according to the location of the sensor nodes. The routing module consists of four sub components such as cluster formation, cluster head selection, routing and trust manager. Here, the sensor nodes are grouped into different groups in cluster formation, a node can be selected as a cluster head according to the trust scores and the energy levels and perform the routing process based on the energy level and the trust scores dynamically.

4 Proposed work

This section is about the proposed routing protocol called Location and Energy Aware Trusted Distance Source Routing (LEATDSR) algorithm for enhancing the performance of the network in terms of improving the network lifetime. This routing protocol is used for identifying the shortest path between the source and sink nodes. Moreover, it is also used to find the alternate route which is the shortest path and also to maintain the route during data communication. The LEATDSR is an energy aware routing and reactive protocol methods which are able to save energy and also works based on the location. Here, it finds the route on demand by flooding the network with data packets route request. In addition, the proposed on demand protocol that is working mainly based on the source-routed on-demand routing which is used for improving the network lifetime. In this network scenario, a sensor node contains route caches with aware source routes when the sensor learns about new route and it updates the entries in the route cache. The effect of standardized wireless sensor networks, the sensor nodes are identical and all of its sensors have the similar storage capacity, processing capability, battery power, sensing ability, and data communication capabilities in the proposed protocol.

4.1 Energy model

The energy model used in this work and its behavior are based on the Equations (1) and (2). The E_{elec}, E_{fs} and ε_{mp} are the electronics energy and the amplifier energy in free space and multipath respectively. The transmission energy needed for an l-bit message more than a separation d is as per the following:

$$E_T(l,d) = \begin{cases} lE_{\text{elec}} + l\varepsilon_{fs}d^2 \text{ for } d < d_0 \\ lE_{\text{elec}} + l\varepsilon_{mp}d^4 \text{ for } d \geq d_0 \end{cases} \tag{1}$$

Where ,$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{mp}}$

The reception energy required for an l-bit message is as follows:

$$E_R(l) = \ l\ E_{elec} \tag{2}$$

The energy utilized by the component of the node operation mode, the reduced energy computation with the component is idle mode for particular time periods. The proposed technique demonstrates that every time a node needs to transmit, it initially identifies the free channel for active data transmission. It also computes the random time for finding the channel.

4.2 Fuzzy temporal rules

The proposed model applies the temporal constraints for taking decision over the sensor nodes which are to be participated in the routing process. Especially, the temporal rules are generated in this work and also incorporated with the fuzzy rules for finalizing the sensor nodes to participate in the routing process in the network according to the distance, trust score, energy and time of the respective nodes. These fuzzy temporal rules are framed by using the trust score levels such as Fair, Medium and Not Fair. Moreover, energy level of the sensor nodes such as Less, Moderate and Acceptable. In addition, the start time and end time are also considered for ensuring the data transmission in a specific path of network.

Rule 1: IF Dist. (i, j) <Th AND Trust = Medium AND Energy = Less AND Start_Time>= T1 AND End_Time<= T2 THEN Node = Normal

Rule 2: IF Dist. (i, j) <Th AND Trust = Fair AND Energy = Moderate AND Start_Time>= T1 AND End_Time<= T2 THEN Node = Cluster Head for small cluster

Rule 3: IF Dist. (i, j)<Th AND Trust = Fair AND Energy = Acceptable AND Start_Time>= T1 AND End_Time<= T2 THEN Node = Cluster Head for large cluster

Rule 4: IF Dist. (i, j)>Th AND Trust = Fair AND Energy = Moderate AND Start_Time>= T1 AND End_Time<= T2 THEN Node = Cluster member for large cluster

Rule 5: IF Dist. (i, j) <Th AND Trust = Not fair AND Energy = Acceptable AND Start_ Time>= T1 AND End_Time<= T2 THEN

Node = Malicious

4.3 Spatial constraints

The proposed protocol uses the spatial constraints for making decision over the sensor nodes. Here, the traffic condition is monitored and also maintained the traffic condition in a specific location of the network for the particular time duration. The traffic condition is monitored in every time interval for the specific location of the network. In this work, spatial manager uses the location and time constraints for providing the facility to predict the network lifetime of sensor nodes in the WSN using the history of traffic conditions. Here, the fuzzy temporal rules are used with the consideration of the location information which is provided by the spatial manager for making effective decision over the malicious node identification and detection process in wireless sensor networks. It also used to select the cluster heads for the network scenario more accurately to utilize the energy of the sensor nodes depends on the time interval. Moreover, it also improves the QoS by increasing the packet delivery ratio and by reducing the delay. Finally, fuzzy logic based spatio-temporal rules have been used in this system for making effective data collection from sensor nodes and takes routing decisions over the sensor nodes in the network.

4.4 Trust model

The proposed trust modelling has been proposed with spatio-temporal features according to the multi-attributes trust modelling, which is proposed for identifying the various types of malicious nodes during the trust score calculation.

4.4.1 Dynamic direct trust

The dynamic direct trust score evaluation is based on the communication speed, the amount of data transmission, energy level, time and the recommendation score which is given by the neighbour nodes in the network. In WSNs, the nodes are coordinating with neighbour nodes and perform the data transmission timely according to the trustworthy[35]. The attackers are always affecting the data transmission, energy and lifetime of the network. Hence, the data communication trust is an important factor for examining the credibility of the neighbour node in the trust evaluation process.

4.4.2 Data communication trust

The data communication trust is useful for detecting the grey-hole and black-hole attacks which are able to affect the data communication process severely in WSNs. The two trust metrics such as packet received and packet forwarding feedbacks have been considered for calculating the direct trust in this work. The packet received feedback is received from the neighbour nodes after received the packets successfully. The data communication process will be considered success when the sender node receives the response from neighbour nodes within the limited time duration. The packet forwarding feedback will be given according to the number of packets are forwarded successfully. The direct trust score is calculated by using the Equation (3).

$$DTS^{i,j} < t_1,\, t_2 >= \frac{SDC^{i,j}+1\ < t_1,\, t_2 >}{\left(SDCT^{i,j}+1\right) < t_1,\, t_2 >\ +\left(UDCT^{i,j}+1\right) < t_1,\, t_2 >} \tag{3}$$

Where DTS^{i,j} indicates the direct data communication trust of the source node i to the destination or neighbour node j. Moreover, SDCT^{i,j} and UDCT^{i,j} denote the total numbers of successful data transmissions and unsuccessful data transmissions between i and j through data communication trust metrics respectively.

4.4.3 Dynamic data trust

Dynamic Data security is an important factor in the security mechanism of any kind of networks. Generally, the different kind of attacks such as compromised forges the data packets and the malicious node partially or completely replaces the original packets which are received from neighbours. For resolving the above mentioned challenges, two data trust metrics have been introduced in this work such as perceived data packet accuracy and data packet accuracy. The perceived data packet accuracy is calculated according to number of data packets have been detected by the neighbour nodes when receives data packet forward request from the source node. If the variation between two data packets is smaller than a certain threshold, then it can be accountable otherwise it is considered as failure. Data packet accuracy is nothing but the neighbour node take backup which data packet sends through this node.

$$DDPT^{i,j} < t_1,\, t_2 > = \frac{SDCT^{i,j}+1\ < t_1,\, t_2 >}{\left(SDCT^{i,j}+1\right) < t_1,\, t_2 >\ +\left(UDCT^{i,j}+1\right) < t_1,\, t_2 >} \tag{4}$$

where DDPT^{i,j} represents the dynamic data packet trust of i to j, while SDCT^{i,j} and UDCT^{i,j} denote the total numbers of successful and unsuccessful data interactions between i and j via data trust metrics respectively.

4.4.4 Dynamic energy trust

Energy trust is an important assessment for enhancing the performance of the wireless sensor network in terms of network lifetime and throughput. Here, the energy consumption process is playing crucial role for enhancing the network lifetime. Moreover, the energy trust computation process can be done by using the energy consumption. In this work, two different energy based trust metrics have been employed as energy ratio and the energy consumption rate. In addition, the energy trust score of the neighbour node is calculated by using the Equation 5.

$$DETS^{i,j} < t_1, t_2 >= \begin{cases} res^t(1-\Delta p)res^t \geq & \varepsilon AND \Delta p \leq v \\ 0 & \mathrm{res}^t < \varepsilon \| \Delta p > v \end{cases} \tag{5}$$

Where DETS^{i,j} represents the energy trust score of i to j during the particular simulation time period.

4.4.5 Recommendation trust measurement

The recommendation trust measurement process is carried out in this work by using the neighbour node recommendation for a node. Here, two kinds of recommendation metrics such as response of the recommendation request and the recommendation accuracy have been employed in this work for calculating the overall recommendation trust score. Here, the response of a recommendation request is checks whether the concern node received the response for the recommendation score from neighbour node. Moreover, the recommendation accuracy is nothing but the score which checks the concern node receives the recommendation data from neighbour node. According to the above two metrics, the dynamic recommendation trust score of the neighbour node is shown as:

$$DRTS^{i,j} < t_1, t_2 > = \frac{SRTS^{i,j} + 1 \ < t_1, t_2 >}{\left(SRTS^{i,j} + 1\right) < t_1, t_2 > \ + \left(URTS^{i,j} + 1\right) < t_1, t_2 >} \tag{6}$$

Where DRTS^{i,j} represents the recommendation trust of i to j during the time duration between t$_1$ and t$_2$, while SRTS^{i,j} and URTS^{i,j}denote the total numbers of successful recommending participation and unsuccessful recommending participation through recommendation trust metrics respectively.

4.4.6 Direct trust score calculation

The direct trust score is calculated by using the sliding window time interval between the node and their neighbour node t$_k$in this work for enhancing the network lifetime. Moreover, the malicious behaviour weight of the node is adopted for comparing the data in each time unit. Here, the dynamic data communication malicious behaviour weight wct$_{tk}$ is expressed in Equation 7.

$$wcts^{t_k} < t_1, t_2 > = maximum \ \left(\alpha_1 \left(1 - \ DCTS^{i,j}_{t=1}\right), \ \alpha_2 \left(1 - \ DCTS^{i,j}_{t=2}\right), \ldots\ldots., \alpha_m \left(1 - \ DCTS^{i,j}_{t=m}\right), \alpha_L \left(1 - \ DCTS^{i,j}_{t=1}\right)\right] < t_1, t_2 > \quad ($$

If the attacker node proceeds a constant but not an understandable attack method so that the anomalous behaviour weight that has been maintained at lower level and also it is an evidently in-adequate to handle such intelligent threat by using the Equation (7). Hence, the attack frequency detection system is required for helping the node i identify whether the neighbour node j is an on-off attacker via data that is recorded in time unit m. Here, consider mc as a unit of communication time that is expressed in Equation 8:

$$m_c < t_1, t_2 >= \begin{cases} \text{normal} & \text{if } DCTS^{i,j}_{t=m} < t_1, t_2 >< \gamma_c \\ \text{abnormal} & \qquad\qquad \text{otherwise} \end{cases} \tag{8}$$

In Equation (8), if the data communication trust score is lesser than a specific threshold c then, the data communication unit (m$_c$) is considered as a normal time unit that is not affected by the malicious attacks in the network, otherwise the data communication unit (mc) is considered as abnormal in this work. After examining the states of all the time units, the attack frequency in sliding window of data communication which is calculated by using the Equation (9):

$$cf^{t_k} < t_1, t_2 > = \frac{ce^{t_k} < t_1, t_2 >}{ce^{t_k} < t_1, t_2 > \ + cn^{t_k} < t_1, t_2 >} \tag{9}$$

Where ce$^t{}_k$$< t_1, \ t_2 >$indicates the total numbers of normal time units and the cn$^t{}_k$ indicates the abnormal time units between the time duration t_1 and t_2. For calculating the weightage of malicious attack and the attack frequency in sliding window time t$_k$, the trust of a neighbour node is calculated by using the Equation 10 in this work.

$$DDCTS^{i,j} < t_1,t_2\rangle = \begin{cases} 1-wct^{t_k} < t_1,t_2 > & \text{if } w\,ct^{t_k} < t_1,t_2 >> cf^{t_k} < t_1,t_2 > \\ \beta\left(1-wct^{t_k}\right) < t_1,t_2 > +(1-\beta)\left(1-cf^{t_k}\right) < t_1,t_2 > \\ \text{otherwise} \end{cases} \tag{10}$$

Where DDCTS^{i,j} indicates the dynamic data communication trust according to the sliding window time $< t_1,\ t_2 >$between the nodes i and j that are a concern node and neighbour node respectively. In equation 8, the malicious behaviour of the neighbour node that are constant in which the values like (wct^{tk}>cf^{tk}). Moreover, the weightage of malicious activity is to be employed in the process of sliding window trust computation. Finally, the direct trust of neighbour node is explained in Equation (11).

$$\begin{aligned} &Td^{i,j} < t_1,t_2 >= \omega_1 DCTS^{i,j} < t_1,t_2 > +\omega_2 DCTS^{i,j} < t_1,t_2 > +\omega_3 ETS^{i,j} < t_1,t_2 > \\ &+\omega_4 RTS^{i,j} < t_1,t_2 > \text{if minimum}\left\{ DCT,j,DCTS^{i,j},ETS^{i,j},RTS^{i,j}\right\} < t_1,t_2 >\geq \mu < t_1,t_2 > \end{aligned} \tag{11}$$

where ω_1, ω_2, ω_3, and ω_4 indicate the weights of two nodes i and j like data communication trust score, direct trust score, energy trust score and the recommendation trust score. Here, the maximum weight of all these trust scores is to be 1and the direct trust score range between1 and 0.

4.4.7 Dynamic indirect trust

The dynamic indirect trust score is nothing but a recommendation score according to the literature survey. According to the principles of indirect trust calculation which indicates the single-hop neighbour nodes of the node and also the neighbour node of the concern node send the direct trust score from node j to node i as recommendation scores. Hence, it is necessary to evaluate the credibility of all the recommendations when the node i receives the recommendation from the G$_{i;j}$. Here, the divergence detection degree (DCi;j) is adopted for analysing such kind of recommendation data in Equation (12).

$$DDC^{i,j} < t_1,\ t_2 >= \frac{\sum \varphi \in G^{i,j} Td^{z,j} +\ \lambda Td^{i,j}}{|G^{i,j}| + \lambda} < t_1,\ t_2 > \tag{12}$$

Where z denotes a node in G$^{i;j}$, while parameter is used for varying the weights of direct trust in divergence detection degree. Moreover, the indirect trust score between the node i and node j of neighbour node, Td is the direct trust and OTd is the indirect trust that is calculated by trust using Equation 13.

$$OTi^{i,j} < t_1,\ t_2 = \frac{\sum \varphi \varepsilon G^{i,j} OTd^{i,z} < t_1,\ t_2 >\ \times OTd^{z,j} < t_1,\ t_2 >}{|G^{i,j}| < t_1,\ t_2 >} \tag{13}$$

4.4.8 Overall dynamic trust score calculation

The overall dynamic total trust score of the neighbour node of any node is calculated by adding the direct trust score and the indirect trust score by using the Equation (14).

$$OTt^{i,j} < t_1,\ t_2 >=\ C^{i,j} Td^{i,j} < t_1,\ t_2 >\ + \left(1 -\ C^{i,j}\right) T_i^{i,j} < t_1,\ t_2 > \tag{14}$$

Where Ci;j indicates the confidence weight of the direct trust in total trust that is calculated by using the Equation (15):

$$C^{i,j} < t_1,\ t_2 > = \frac{N_i^{i,j} < t_1,\ t_2 >}{N_i^{i,j} < t_1,\ t_2 > +n} \tag{15}$$

where$N_i^{i,j} < t_1,\ t_2 >$indicates that the total number of direct interactions, while parameter n is a positive integer, whose value affects the variation rate of C$^{i;j}$$< t_1,\ t_2 >$.By using the equations (12) and (13), it is worth pointing out that the necessity of indirect trust depends entirely on the confidence weight of direct trust. As time wears on, the increasing number of direct interactions between subject and object node brings about the declining proportion of indirect trust in total trust, which enhances network security against recommendation-targeting attacks to some extent.

4.5 Location and energy aware trusted distance source routing

Moreover, the proposed secure routing protocol which is capable of choosing the best cluster and the cluster heads that has the sufficient energy and trustworthiness. Here, cluster head selection is based on the identical connected nodes, the maximum number of sensor nodes and their residual energy level. The proposed routing protocol consists of two different phases such as route discovery and route maintenance. Moreover, the route cache is verified first and then transmits the data packets from source to destination. In this scenario, if the proposed protocol identifies the presence of unexpired route which is used to start the route discovery process. This route identification is done by sending a route request data which contains the address, source, destination and the unique number for identification[14]. Here, the identification node checks the possible route to reach the right destination from source node. In case, not able to identify the right route then the current node address is to be added as one of the information over the route record and forward it to the neighbour nodes. Moreover, the nodes forward only the route request packet which has not seen early and the not available in the route record of the data packet without address. It is useful for limiting the number of route requests. In WSNs, energy efficiency can be acquired through the reliable energy dissipation and also balance the quality of data by using the protocol. Figure 2 demonstrates the flowchart for the algorithm and the steps of the proposed Location and Energy aware Trusted Distance Source Routing (LEATDSR) algorithm are as follows:

Location and energy aware t rusted distance source routing (LEATDSR) algorithm

Input : Sensor nodes data

Output : Secured Routes with the sufficient residual energy

```
Step 1: Data Packet is sent to the concern source node
Step 2: If the source node accepts the data packet then initialize the request for data transmission.
Step 3: Confirm the destination for the route cache.
Step 4: If the destination is identified then
Sends the data
Else
Start the route discovery process with the consideration of the trust scores such as dynamic data communication trust, dynamic data trust and dynamic recommendation trust.
Step 5: Source node identifies their location of their destination.
Step 6: Source node sends the data after identifying the location of route cache and start the route discovery process further.
Step 7: Route Request data packet transmission is processed through the header of Route Request <SID, DID>
Step 8: The source node will send the route request data packet when the process of route discovery started and it can be sent through route request header.
Step 9: Each sensor node contains the parameters are Node_ID
Node Energy Trust(NET)
Node EnergyTrust is followed by:
If (NET <30%)
Then Set NET = 1
If (30% <=NET<= 70%)
Then Set NET = 2
If (NET<70%) Then
Set NET = 3
Energy level is updated at each node
Parameters Unease while Searching the Route
Step 10: The source node uses the various parameters for reaching the destination node with Node-ID and Node Energy.
Step 11: The Total Node Energy is used for identifying the node which is maintaining the similar amount of energy and also the dead nodes are present in the deployed sensor networks. [TNET (Total Node Energy Trust), NMNs (Number of Malicious Nodes) and Node_ID]
Step 12: The following parameters are used the proposed model is in order to reach the destination apart from Node ID and Node energy: Malicious nodes, Total Node Energy (Alive Node)
Step 13: Hence, the Node Energy Trust and Total Node Energy Trust Score is evaluated by,
If (NET == 3) Then
TNET = TNET + 3
Else-if (NET == 2) Then
TNET = TNET + 1
Else-if (NET == 1)
```

MN's= MN's + 1

Step 14: Here, MN's indicates a Malicious Nodes and it has > 30% energy.

Step 15: To calculate the number of malicious nodes present in the sensor field,if the node energy range is equal to 3, it means that the specified node is Malicious Node. If the range goes below 3, it is not Malicious Node.

Step 16: Destination node ensures the route and searches the route which has smallest weedy nodes after threshold time T.

Step 17: After identifying the energy level, the destination node finds the route according to the trust worthiness. The process of finding the route is based on the smallest weedy node after the threshold and the spatial and temporal constraints.

Step 18: Finally the node with more energy is taken out if not there is a need of changing the condition,

Step 19: If (HC (path (PADSR))>HC (path (DSR))) Then Select_Path (PADSR)

Step 20: At last, the node energy which has more amount of energy is taken out. If there are no such nodes the condition is modified.

Step 21: Call K-Means clustering algorithm with the consideration of energy and Energy Trust Scores of the participated nodes.

Step 22: Apply Spatial and temporal constraints over the participating nodes in the network scenario.

Step 23: Perform routing operation according to the energy and trust worthiness of nodes.

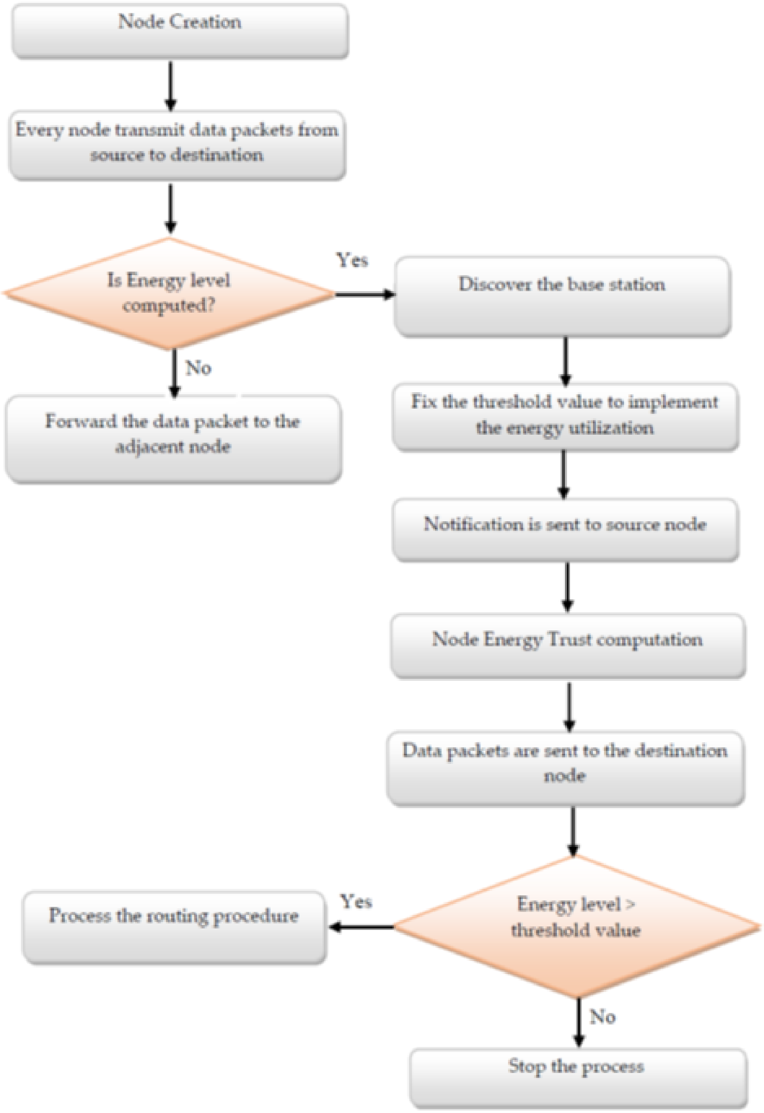
Node Creation
Every node transmit data packets from source to destination
Is Energy level computed?
Yes
No
Discover the base station
Forward the data packet to the adjacent node
Fix the threshold value to implement the energy utilization
Notification is sent to source node
Node Energy Trust computation
Data packets are sent to the destination node
Process the routing procedure
Yes
Energy level > threshold value
No
Stop the process

Fig 2. Performance analysis of Black and Grey-hole attacks detection

5 Results and discussion

The proposed model has been implemented by using NS-2 simulation tool. The efficiency of the proposed model has been proved that by conducting various experiments by considering the time, transmission rate, throughput, latency and the presence of malicious nodes in the wireless sensor network. Moreover, the performance of the proposed Location aware Energy trusted secure routing algorithm is performed well in terms of end-to-end delay, throughout, average latency time, routing overhead and the network lifetime. Table 1 shows that the simulation parameters which are used in the simulation.

Table 1. Simulation parameters.

Parameter	Value
Simulation Time	500s
Monitoring Area	200m X 200m
Number of sensor nodes	100
Proportion of malicious nodes	20%
Deployment of sensor nodes	Random
Physical propagation model	Two-way ground reflection
MAC Layer protocol	IEEE 802.14.4
Transport layer protocol	LDTS (Li et al 2013)
Communication range	50m
Length of packet	100 bytes
Local storage	50KB
Initial Energy	25J

Figure 3 shows the performance of the proposed model in the detection of black hole attack and grey hole attach which are able to receive the data packets while transmitting / forwarding to the neighbour nodes in the wireless sensor networks. Here, we have considered the average data packet transmission rate in various simulation times.

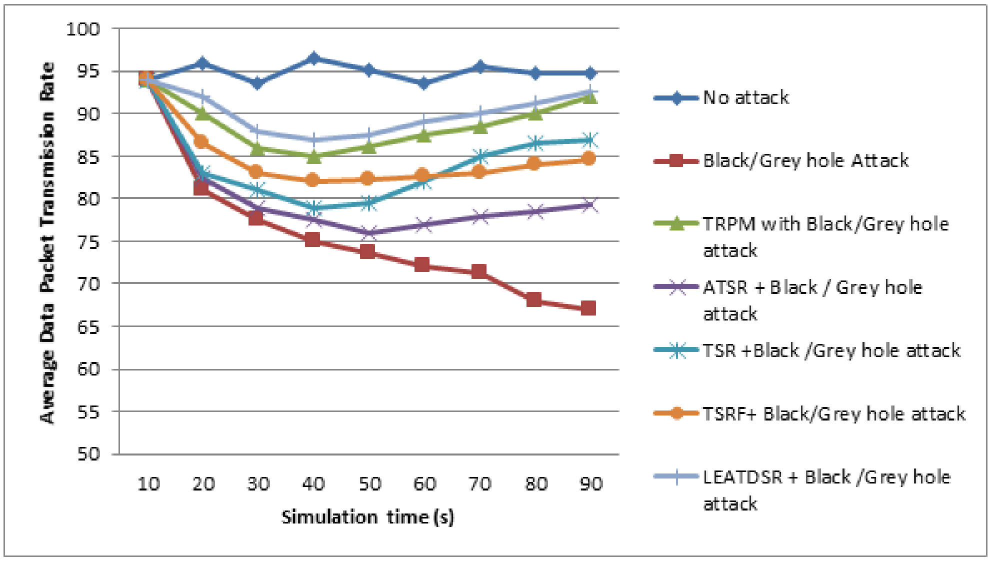

Fig 3. Performance analysis of Black and Grey-hole attacks detection

From Figure 3, it can be seen that the performance of the proposed Location and Energy aware Trusted distance source routing (LEATDSR) algorithm based on the data packet transmission rate is performed well over the detection of black-hole attacks and grey-hole attacks when it is compared with the other existing algorithms such as Trusted Aware Routing Protocol with Multi-attributes (TRPM), Ambient Trust Sensor Routing solution (ATSR), Trust based Source Routing (TSR) and Trust-aware Security Routing Framework (TSRF)[36]. This is due the fact that the use of effective trust modelling and monitoring the energy level continuously and spatial constraints.

Figure 4 shows the performance of the proposed model in the detection of tamper attack which is able to damage the data packets while transmitting / forwarding to the neighbour nodes in the wireless sensor networks. Here, we have considered the tamper attack detection rate in various simulation times.

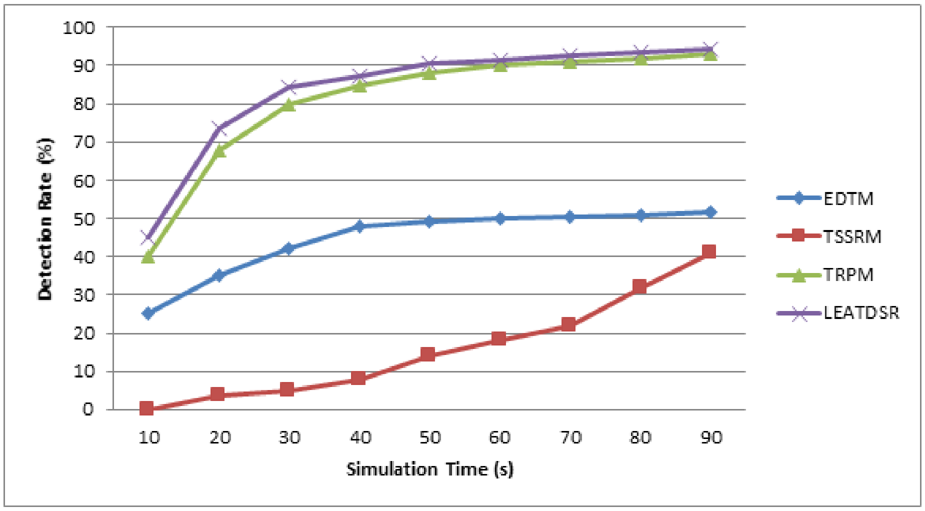

Fig 4. Performance over the tamper attack detection in different simulation time

From Figure 4, it can be observed that the performance of the proposed LEATDSR algorithm is performed well over the detection of tamper attack detection when it is compared with the existing algorithms such as Efficient Distributed Trust Model (EDTM), TSSRM and TRPM. This is due the fact that the use of effective trust modelling and monitoring the energy level continuously and spatial constraints.

Figure 5 shows the performance of the proposed model in the detection of tamper attack which is able to damage the data packets while transmitting / forwarding to the neighbour nodes in the wireless sensor networks. Here, we have considered the tamper attack detection rate in various simulation times.

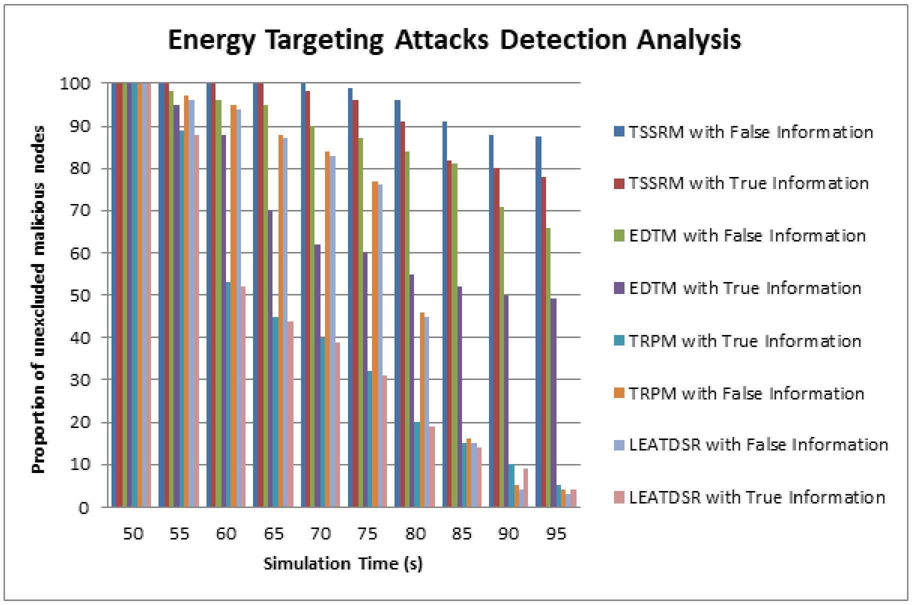

Fig 5. Performance analysis over the energy targeting attacks

From Figure 5, it can be observed that the performance of the proposed LEATDSR algorithm is performed well over the detection of energy targeted attack detection when it is compared with the existing algorithms such as TSSRM, EDTM and

TRPM with true and false information. This is due the fact that the use of effective trust modelling and monitoring the energy level continuously and spatial constraints.

Figure 6 shows the variation of average data packet transmission rate with the increase of proportion of malicious behaviours. Here, we have considered the data packet transmission rate for the transactions which are transmitted in various time period.

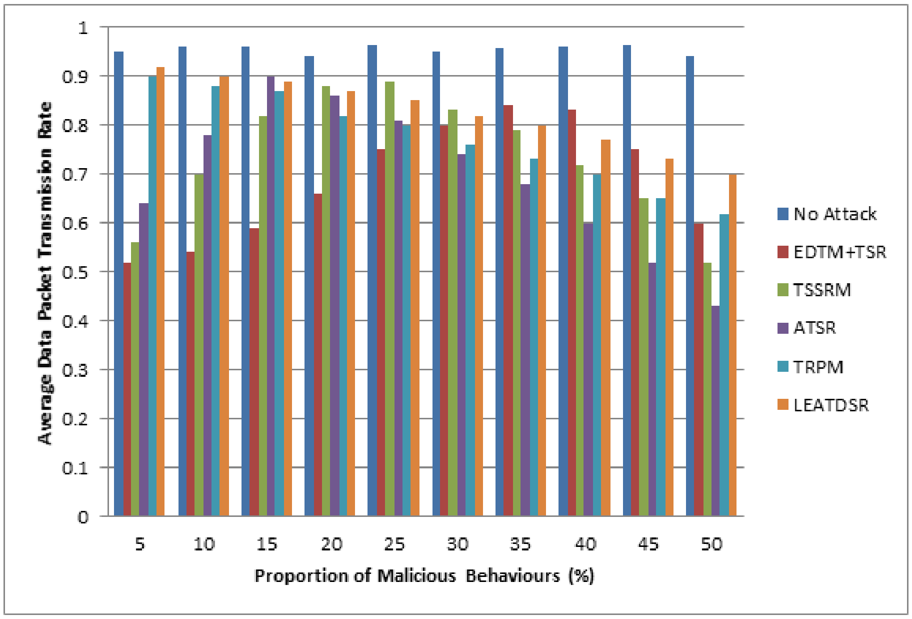

Fig 6. Performance analysis of detecting malicious attacks

From Figure 6, it can be seen that the performance of the proposed LEATDSR algorithm is perform well over the detection of malicious nodes in the network when it is compared to the other existing algorithms such as TRPM, ATSR, TSSRM and EDTM with TSR that are available in this direction. This is due the fact that the use of effective trust modelling and monitoring the energy level continuously and spatial constraints. The main objective of the proposed location and energy aware trusted distance source routing algorithm is to detecting the multi-nature malicious attacks.

Figure 7 shows the throughput analysis between the proposed LEATDSR algorithm and the existing models such as TPR, TSSRM, TSRF and TSR. Here, six different experiments have been conducted for finding the average throughput when uses the different numbers of malicious nodes such as 5, 10, 15, 20 and 25.

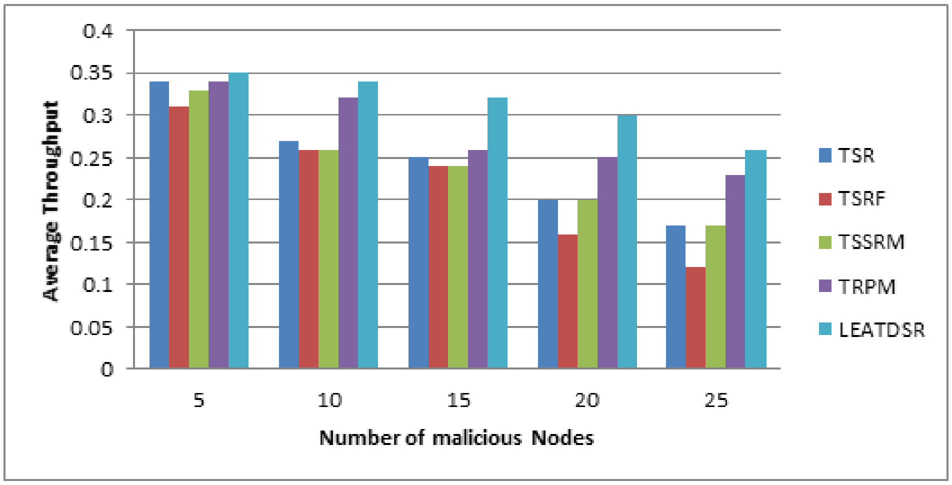

Fig 7. Throughput Analysis

From Figure 7, it can be observed that the performance of the proposed LEATDSR algorithm
is better when it is compared with the other existing systems such as TRPM, TSSRM, TSRF and TSR. In all the five experiments also performed well due to the use of effective trust modelling, consideration of energy, sliding window time and the location of the nodes.

Figure 8 shows the average end-to-end latency analysis between the proposed LEATDSR algorithm and the existing models such as TPR, TSSRM, TSRF and TSR. Here, six different experiments have been conducted for finding the average end-to-end latency when uses the different numbers of malicious nodes such as 5, 10, 15, 20 and 25.

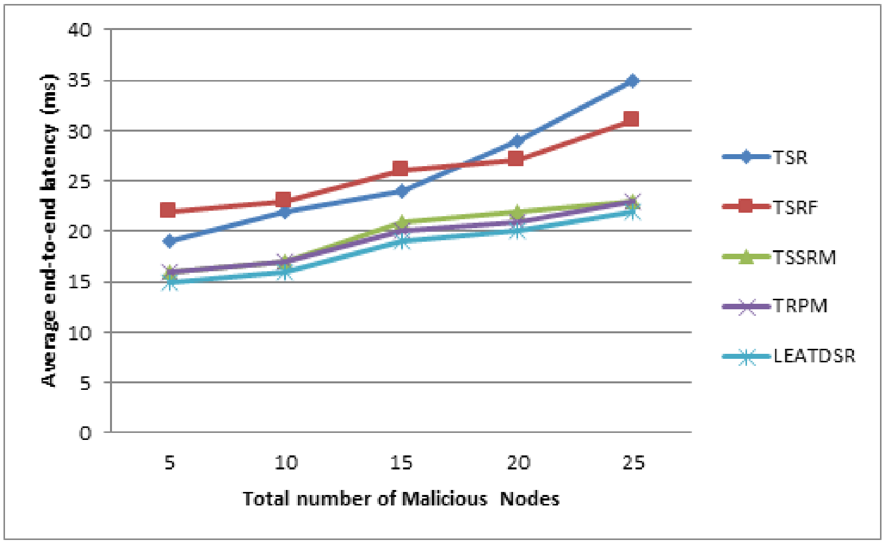

Fig 8. Average end-to-end latency analysis

From Figure 8, it can be observed that the performance of the proposed LEATDSR algorithm is better when it is compared with the other existing systems such as TRPM, TSSRM, TSRF and TSR. In all the five experiments also performed well due to the use of effective trust modelling, consideration of energy, sliding window time and the location of the nodes.

Figure 9 shows the throughput analysis between the proposed LEATDSR algorithm and the existing models such as TPR, TSSRM, TSRF and TSR. Here, five different experiments have been conducted for finding the average throughput when uses the different numbers of malicious nodes such as 5, 10, 15, 20 and 25.

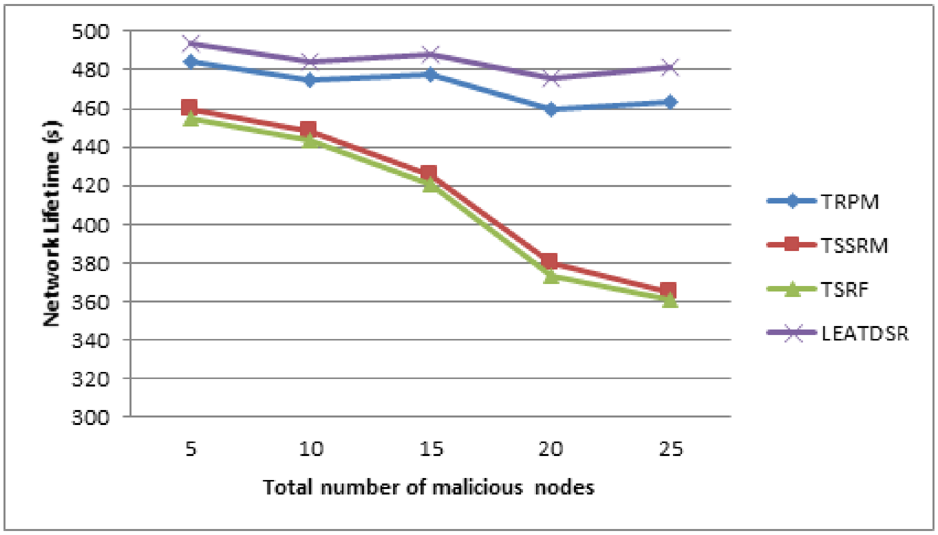

Fig 9. Network lifetime analysis

From Figure 9, it can be observed that the performance of the proposed LEATDSR algorithm is better when it is compared with the other existing systems such as TRPM, TSSRM and TSRF. In all the five experiments also performed well due to the use of effective trust modelling, consideration of energy, sliding window time and the location of the nodes.

The proposed technique could access the local energy and the global energy that the interpretation of the analysis to obtain the consumed energy by a sensor node and the energy which depends on the total amount of packets are communicated in the network. The black and grey-hole attacks detection process is completed by the proposed technique and it has the enhanced detection rate than the methods of TSRF, TSR, ATSR and TRPM. The detection rate for the proposed LEATDSR has around 45% to 93% and other techniques such as EDTM has 24% to 52%, TSSRM has 2% to 41% and TRPM has 38% to 91%. The average data packet transmission rate for the proposed LEATDSR is higher value compared with other methods. The average throughput despite total amount of malicious nodes for the proposed technique has the highest value than the techniques of TSRF, TSR, ATSR and TRPM. The proposed technique has the reduced average end-to-end latency and enhanced network lifetime than the related techniques.

6 Conclusion and future work

A new energy efficient secure routing algorithm called Location and Energy Aware Trusted Distance Source Routing (LEATDSR) algorithm has been proposed and implemented in this work for enhancing the network life time and the QoS of WSNs. In this algorithm incorporates a new trust modelling which has various attributes over the trust score calculation for identifying the black-hole and grey-hole attacks while transmitting the data packets. Before that, energy level also monitored for ensuring the participation over the routing process. Before start the data communication in WSNs, dynamically calculates the data packet trust and the data packet communication trust for reliable communication. In addition, the existing k-means clustering algorithm has been used for grouping the nodes according to the location of nodes which are eligible to participate in the routing process. Finally, the experimental results proved that the performance of the LEATDSR algorithm in terms of QoS and the network life time in WSNs. The common functionality of a WSN is forwarding data to the adjacent node and identifying the channel to discover the optimized routing, some of the nodes into the passive mode to consume the minimum energy in the network. Further works can be done in this direction by the use of intelligent agents for effective data communication.

References

1) Sun B, Li D. A comprehensive trust-aware routing protocol with multi-attributes for WSNs. *IEEE Access*. 2018;6:4725–4741. Available from: https://dx.doi.org/10.1109/access.2017.2786944.
2) Butun I, Morgera SD, Sankar R. A Survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*. 2014;16(1):266–282. Available from: https://dx.doi.org/10.1109/surv.2013.050113.00191.
3) Mini RAF, do Val Machado M, Loureiro AAF, Nath B. Prediction-based energy map for wireless sensor networks. *Ad Hoc Networks*. 2005;3(2):235–253. Available from: https://dx.doi.org/10.1016/j.adhoc.2004.07.008.
4) Ishmanov F, Malik AS, Kim SW, Begalov B. Trust management system in wireless sensor networks: design considerations and research challenges. *Transactions on Emerging Telecommunications Technologies*. 2015;26(2):107–130. Available from: https://doi.org/10.1002/ett.2674.
5) Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song YJ. Group-Based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*. 2009;20(11):1698–1712. Available from: https://dx.doi.org/10.1109/tpds.2008.258.
6) Yu H, Shen Z, Miao C, Leung C, Niyato D. A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE*. 2010;98(10):1755–1772. Available from: https://dx.doi.org/10.1109/jproc.2010.2059690.
7) Govindan K, Mohapatra P. Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials*. 2012;14(2):279–298. Available from: https://dx.doi.org/10.1109/surv.2011.042711.00083.
8) Muthurajkumar S, Ganapathy S, Vijayalakshmi M, Kannan A. An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs. *Wireless Personal Communications*. 2017;96:1753–1769. Available from: https://dx.doi.org/10.1007/s11277-017-4266-4.
9) Naranjo PGV, Shojafar M, Mostafaei H, Pooranian Z, Baccarelli E. P-SEP: a prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks. *The Journal of Supercomputing*. 2017;73(2):733–755. Available from: https://dx.doi.org/10.1007/s11227-016-1785-9.
10) Khan BM, Bilal R, Young R. Fuzzy-TOPSIS based cluster head selection in mobile wireless sensor networks. *Journal of Electrical Systems and Information Technology*. 2017;p. 1–16. Available from: https://doi.org/10.1016/j.jesit.2016.12.004.
11) Shokouhifar M, Jalali A. Optimized sugeno fuzzy clustering algorithm for wireless sensor networks. *Engineering Applications of Artificial Intelligence*. 2017;60:16–25. Available from: https://dx.doi.org/10.1016/j.engappai.2017.01.007.
12) Mirzaie M, Azinan S. MCFL: an energy-efficient multi-clustering algorithm using fuzzy logic in wireless sensor network. *Wireless Networks*. 2017;p. 1–16. Available from: https://doi.org/10.1007/s11276-017-1466-5.
13) Ahmed A, Bakar KA, Channa MI, Haseeb K, Khan AW. A trust aware routing protocol for energy constrained wireless sensor network. *Telecommunication Systems*. 2016;61(1):123–140. Available from: https://dx.doi.org/10.1007/s11235-015-0068-8.
14) Liu Y, Dong M, Ota K, Liu A. ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*. 2016;11(9):2013–2027. Available from: https://dx.doi.org/10.1109/tifs.2016.2570740.
15) Zahariadis T, Trakadas P, Leligou HC, Maniatis S, Karkazis P. A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks. *Wireless Personal Communications*. 2013;69:805–826. Available from: https://dx.doi.org/10.1007/s11277-012-0613-7.

16) Xia H, Jia Z, Li X, Ju L, Sha EHM. Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks*. 2013;11(7):2096–2114. Available from: https://dx.doi.org/10.1016/j.adhoc.2012.02.009.

17) Ayyasamy A, Venkatachalapathy K. Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs. *Wireless Networks*. 2015;21:421–430. Available from: https://dx.doi.org/10.1007/s11276-014-0801-3.

18) Jiang J, Han G, Wang F, Shu L, Guizani M. An Efficient Distributed Trust Model for Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*. 2015;26(5):1228–1237. Available from: https://dx.doi.org/10.1109/tpds.2014.2320505.

19) Tamilselvan S, Venkatachalapathy K, Ayyasamy A. An Efficient Energy Conservation using Diffusion Update Algorithm in Wireless Sensor Networks. *International Journal of Control Theory and Applications*. 2016;9(2):521–529. Available from: https://serialsjournals.com/abstract/69814_14.pdf.

20) Thirukrishna JT, Karthik S, Arunachalam VP. Revamp energy efficiency in Homogeneous Wireless Sensor Networks using Optimized Radio Energy Algorithm (OREA) and Power-Aware Distance Source Routing protocol. *Future Generation Computer Systems*. 2018;81:331–339. Available from: https://dx.doi.org/10.1016/j.future.2017.11.042.

21) Airehrour D, Gutierrez JA, Ray SK. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Generation Computer Systems*. 2019;93:860–876. Available from: https://dx.doi.org/10.1016/j.future.2018.03.021.

22) Wang R, Zhang Z, Zhang Z, Jia Z. ETMRM: An Energy-efficient Trust Management and Routing Mechanism for SDWSNs. *Computer Networks*. 2018;139:119–135. Available from: https://dx.doi.org/10.1016/j.comnet.2018.04.009.

23) Logambigai R, Ganapathy S, Kannan A. Energy–efficient grid–based routing algorithm using intelligent fuzzy rules for wireless sensor networks. *Computers & Electrical Engineering*. 2018;68:62–75. Available from: https://dx.doi.org/10.1016/j.compeleceng.2018.03.036.

24) Mythili V, Suresh A, Devasagayam MM, Dhanasekaran R. SEAT-DSR: Spatial and energy aware trusted dynamic distance source routing algorithm for secure data communications in wireless sensor networks. *Cognitive Systems Research*. 2019;58:143–155. Available from: https://dx.doi.org/10.1016/j.cogsys.2019.02.005.

25) Xu C, Xiong Z, Zhao G, Yu S. An Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN. *IEEE Access*. 2019;7:135277–135289. Available from: https://dx.doi.org/10.1109/access.2019.2942321.

26) Haseeb K, Abbas N, Saleem MQ, Sheta OE, Awan K, Islam N, et al. RCER: Reliable Cluster-based Energy-aware Routing protocol for heterogeneous Wireless Sensor Networks. *PLOS ONE*. 2019;14(9). Available from: https://dx.doi.org/10.1371/journal.pone.0222009.

27) Ketshabetswe LK, Zungeru AM, Mangwala M, Chuma JM, Sigweni B. Communication protocols for wireless sensor networks: A survey and comparison. *Heliyon*. 2019;5. Available from: https://dx.doi.org/10.1016/j.heliyon.2019.e01591.

28) Tang L, Lu Z, Fan B. Energy Efficient and Reliable Routing Algorithm for Wireless Sensors Networks. *Appl Sci*;2020. Available from: https://doi.org/10.3390/app10051885.

29) Rajeswari AR. A Mobile Ad Hoc Network Routing Protocols: A Comparative Study. *Recent Trends in Communication Networks*. 2020. Available from: https://doi:10.5772/intechopen.92550.

30) Shafiq M, Ashraf H, Ullah A, Tahira S. Systematic Literature Review on Energy Efficient Routing Schemes in WSN – A Survey. *Mobile Networks and Applications*. 2020;25(3):882–895. Available from: https://dx.doi.org/10.1007/s11036-020-01523-5.

31) Rodríguez A, Del-Valle-Soto C, Velázquez R. Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks Based on Yellow Saddle Goatfish Algorithm. *Mathematics*. 2020;8(9):1515–1515. Available from: https://dx.doi.org/10.3390/math8091515.

32) Del-Valle-Soto C, Velázquez R, Valdivia LJ, Giannoccaro NI, Visconti P. An Energy Model Using Sleeping Algorithms for Wireless Sensor Networks under Proactive and Reactive Protocols: A Performance Evaluation. *Energies*. 2020;13:3024–3024. Available from: https://dx.doi.org/10.3390/en13113024.

33) Li H, Liu S, Hu B. Research on Node Sleep/Wake-up Mechanism in WSN Based on Energy Threshold Setting. In: 5th International Conference on Wireless Communications, Networking and Mobile Computing. 2009;p. 1–4. Available from: https://doi.org/10.1109/WICOM.2009.5304258.

34) Hady AA, El-kader SMA, Eissa HS. Intelligent Sleeping Mechanism for wireless sensor networks. *Egyptian Informatics Journal*. 2013;14(2):109–115. Available from: https://dx.doi.org/10.1016/j.eij.2013.03.002.

35) Han G, Jiang J, Shu L, Niu J, Chao HC. Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*. 2014;80(3):602–617. Available from: https://dx.doi.org/10.1016/j.jcss.2013.06.014.

36) Duan J, Yang D, Zhu H, Zhang S, Zhao J. TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2014;10(1). Available from: https://dx.doi.org/10.1155/2014/209436.