A trusted approach for prediction of data link failure and intrusion detection in wireless sensor networks

Putty Srividya (srividyaosmania@gmail.com)
Osmania University
Lavadya Nirmala Devi
Osmania University
Nageswar Rao A
Hindustan Aeronautics Limited

Research Article

Keywords: WSN, Posterior probability estimation, PTN-RRP, Weighted end-to-end delay, Link failure, attack estimation

Posted Date: September 15th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-903992/v1

A TRUSTED APPROACH FOR PREDICTION OF DATA LINK FAILURE AND INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

Putty Srividya[1]and Dr. Lavadya Nirmala Devi[2] and Dr A Nageswar Rao[3]

[1]Assistant Professor, [2]Professor, [3]Senior Manager
[1,2]Dept. ECE, University College of Engg.
[1,2]Osmania University, Hyderabad, India.
[3]HAL,Hyderabad, India

Email: [1]srividyaosmania@gmail.com, [2]nirmaladevi@osmaina.ac.in and [3]nagiitkgp@gmail.com

Abstract. Typically, wireless senor network (WSN) is widely used in the various fields for several applications. It is a promising technology due to its higher range of the network connectivity and the fast set up of the network. But there will also be a presence of the some of the eradicating issues which will decrease the network growth. In the WSNfield the prediction of link failure is regarded as the baffling one till now. The proposed technique offers a detailed idea on the failure of link. The proficient trusted Node ID dependent resource reservation protocol (PTN-RRP) is presented in this approach. In this, the shortest path is then recognized with the use of approach weighted based end-to-end delay. This technique identifies the shortest path from a specific preliminary position to the target and thus could enhance the detectionrate. By means of recognizing shortest path, the hop address and sequence numeral is being incorporated to the protocol. Once afterwards the shortest pathdetection, the failure of link is estimated. A link failure structure in the trusted etiquetteemployed has the developedcapabilityto predict and fix issues related to link failure. After that, to identify the attack cause intended for the failureof link, a method of posterior probability evaluation is carried out to find the kind of attack. Finally, the proposed method performance isassessedover simulation study. The simulation outcomeauthorizes that the projectedmethod is effective highly in the link breakage detectionand the implemented algorithm for shortest path recognition in this will decreases the detecting shortest path time period. The performance outcome is compared with existing techniques to prove the effectiveness of proposed methodology**.**

***Index Terms*—**WSN, Posterior probability estimation, PTN-RRP, Weighted end-to-end delay, Link failure, attack estimation.

1. Introduction

Wireless Sensor Networks (WSNs) incorporate sensor nodes and is capable of communicating with other devices through radio modules or base station and is having the known characteristics such as less battery power [1], limited storage capacity, and low computational capacity that are deployed to sensing the data collection and data communication [2]. Conversely, the sensor nodes route the data collection through their intermediate nodes that are connected through wireless sensors, to send the data to the receiver node[3]. The incorporation of both Software Defined Networking (SDN) and Cloud Computation model in turn automates theapplications provisioning along with heterogeneous networks in the cloud in the course of programmable vertical interface. This technological incorporation enhances themanagement ofresource efficiently, controllability, and network extensibility, scalability dynamically intended for fast and enhanced communication. Therefore, the conventional cloudcomputation was altered to the enriched platform of service-delivery over the pool of Software Defined controllers.

Since the communication gets complicated, the communicationstrategies turn out to be susceptible to the several number of attack types [4]. These attacks were crafted ambitiously intended for a denial of any service cause throughout the networkcongestion, demanding the memoryprocessor, thereby decreasing the computational power, the timing data communication disruptingcomprise their own limitationresource, several operating system introductions in the connecting sensors. In spite of their restrictions, the requirement of huge data capacity storage along with the use of battery in the hand-held sensors [5]. In several circumstances, the distributed networking surroundings through the impersonationof cloud framework, these become a cause for escalating the

security threats. So as to stabilize high technological development in the infrastructure of networking and intelligencehacking together, appropriate techniques and mechanisms were integrated forencountering the data privacy and security attacks[6]. The scenario of networking must be strengthen with standard privacy and security policy for a safe communication[7, 8].

The presence of malicious nodes may fall in the packets intentionally or misguide the messages in the routes or the active packets routing to be repeats from the standardized sensor nodes to the believable neighbor nodes that followed by the Cluster Heads that have the highest trust for efficient secured WSN routing process. By considering this, the high trust values from the Cluster Heads to be selected that depends upon for the attacking nodes prevention from the Cluster Head[9]. However, to isolated the malicious nodes from various Cluster Members also for the illegal activities to be reducing and the tampering activities to be avoiding in the network that leads to trust values-based accuracy reduction. By consider the cluster-based routing method, the Cluster Head that collects the data from its respective member nodes, aggregates it and transmits the collection of data to the receiver through the way of single-hop or multi-hop routing method.The approach of multi-hop routing gives a chance for the nodes to show the malicious node activities that have in the WSNs[10, 11]. Due to the existence of malicious nodes, the necessary secure routing protocols and its design issue have in Wireless Sensor Nodes[12]. The presence of malicious nodes may fall in the packets intentionally or misguide the messages in the routes or the active packets routing to be repeats from the standardized sensor nodes to the believable neighbor nodes that followed by the Cluster Heads that have the highest trust for efficient secured WSN routing process.

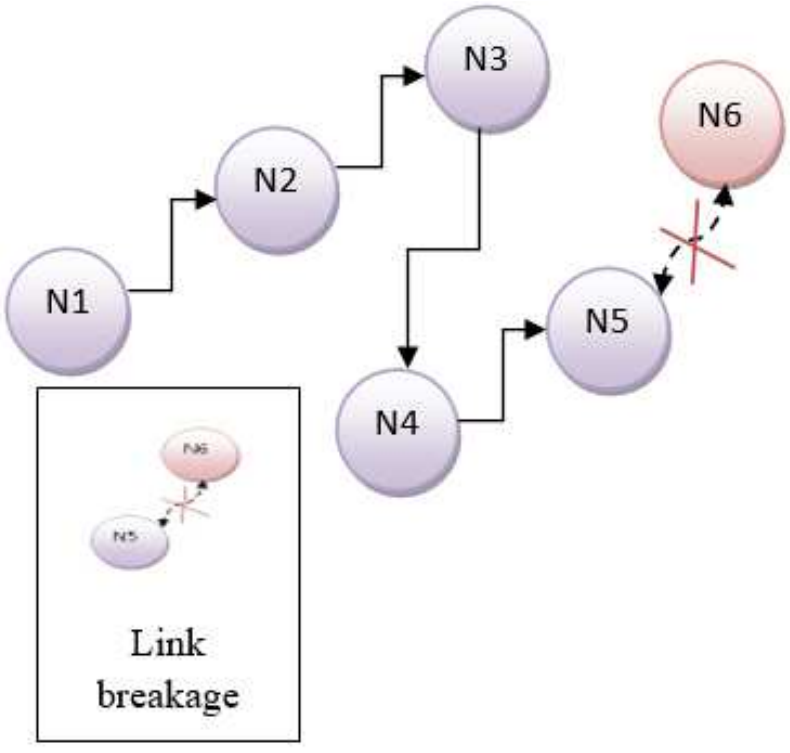

Figure:1 representation of breakage of link among the nodes

Formerly the nodes will be goneinaccessiblesome time for the reason of failure in the link. This failure kind might lead to the irregularity formation in the process. There were 2failure kinds mainly in WSN, they are: the failure occurred in the middle of communication link and failure in more than one node. Typically, the failure in

the link may cause the reduction of throughput and in turn leads to the network growth deduction.Inappropriately, there will be nothing other actualanalysistechnique for the link failure detection. In some other prevailingmethods, the researchers mostly emphasis on the attack detection and themalicious node. There would be fewrestrictedlearningaffiliatedto the analysis of link failure. This couldpersuade the investigators to progressanextremelydependableconstructionintended forthe prediction of link failure.

The overall organization of the paper as given below: Section 2 offers the related works about the trust approach for data link failure over several authors point of view. Section 3 provides the detailed explanation about the proposed methodology with its respective operation. Section 4 describes the performance analysis about the proposed work with the existing methods in comparison manner. Section 5 concludes the paper with effective description.

2. Related Works

[13] Highlighted the challenges of application met by WSNs for monitored environment and those met by the suggested techniques, in addition to chance that could be exposed on WSNs applications with SDN. Also, Implementation considerations were highlighted by focusing vital aspects that could not be ignored while enhancing network functionalities. A strategy for Software Defined Wireless Sensor Network (SDWSN) was presented as an attempt for enhancing application in monitored frameworks.

[14] developed an assuring security scheme for WSN, so as to pact with these kinds of attacks in multicasting and unicasting. In this work, the detection and prevention of Sybil attack was done with the use of passing and message authentication method. The Sybil attack was a huge disparaging attack aligned with the sensor network wherever many real identities along with fake id's was employed for receiving an illegal access to network system.

[15] projected a method which was not in favor of sinkhole attacks and identifies malicious nodes with the use of hop counting. The major benefit of the projected method was that, a node was capable of identifying malicious nodes in collaboration with neighbor nodes devoid of requiring any concession with BS (base station). False detection of attacks was the major limitation of this wok.

[16] Proposed a modern on-demand trust-based unicast routing protocol for MANETs, called the TSR, offers a versatile and workable solution to selecting the shortest path for packet transmission that is best safeguarded.A protocol for complex trust protection is presented in the presence of well-composed, greedy and malicious nodes to secure optimization route in DTN environments. We are designing and validating a modern model-based approach to evaluating and simulating our trust procedure. In addition, we approach dynamic trust management, i.e., in reaction to rapidly shifting network circumstances, in order to reduce faith and optimize routing appliance efficiency, the determination and implementation of the right operating settings at runtime.

[17] Proposes a hybrid metric trust based on the principle of social trust and the QoS. Routing Protocol Adhoc on-demand distance vectors (AODVs) is expanded, and the trust-based paradigm is fused with a process of discovery for the attack patterns so as to lessen opponents' ability to perform various kinds of packet forwarding malpractice.

[18]a distributed intrusion detection scheme (IDS) was developed for the prevention and detection of Gray hole attack in WSN. Flooding attack was considered to be the major one in consuming maximum sensor node battery life among various DoS attacks. Conversely the attack Gray hole consumes the reduced rate of node's battery life. Therefore, as per the energy, these attacks were isolated and distinguished from the network with the use of proposed IDS by carrying out extensive outcomes with the use of NS2- MANNASIM structure. The detection

accuracy is lower and is the major downside of this method.

[19] presented a work on security improvement in wireless sensor networks (WSN) over the reluctant checksum. It was described that from wireless security perspective, it is difficult to incorporate checksum series in the frame of information link layer with no safety. A hesitant checksum system termed R-CS was projected. As per the intrinsic feature of wireless networks error of that frame was predictable, frame's checksum was confined through R-CS accumulated checksum algorithm. The frame's checksum will not be decoded by means of every node apart from the receiver side. Exclusive of checksum, defenders cannot differentiate correct ones from error frames. RCS needs small communication and computation sources, which was appropriate on the whole for resource-limited WSN. The outcomes demonstrate obviously that R-CS was viable for WSN.

[20]presented a wormhole attack that was considered as the challenging task in the adhoc networks and predominantly a tedious task for defending purpose. The wormhole attack is feasible however the host was not negotiated through the attacker, and though communication altogether offers authenticity and confidentiality. In the wormhole attacks, this deteriorates the performance gainof network coding. A WSN has huge sensor nodes with restricted batteries; to collect data the sensor nodes were randomly deployed on a zone. This work was employed to focus the impact of wormhole recognition and deterrence by diverse kinds of improvement technique.

[21] described the Countermeasures and Attacks linked to WSN security issues. WSN are one of the most challenging and exciting domains of research at this time. Due to the aggressive nature of their exploitation surrounding, the wireless medium and the constrained resource nature on the small sensor nodes employed in such networks, security cause more rigorous challenges on comparing conventional networks. As attacks to some hardware or software part might offer important network damages. Certainly, the growth of efficient and effective security method to those attacks has to be addressed at each system design phase.

[22]projected a viewpoint on the NIDS (Network Intrusion Detection Systems), predominantly signature-dependentNIDSs, were positioned in the distributed network environment extensively to protect not in courtesy of a system attacks range.

[23] Proposed an Ad-hoc Routing (T2AR) Trust-aware protocol measuring the Trust Level between the MANET nodes and conducting the safe transfer of data between nodes. It predicts a value of confidence dependent on distance calculation of electricity, mobility and RSSI. This Protocol offers neighbor information about packet transmission's success and failure rates. [17] Proposes a hybrid metric trust based on the principle of social trust and the QoS. Routing Protocol Adhoc on-demand distance vectors (AODVs) is expanded, and the trust-based paradigm is fused with a process of discovery for the attack patterns so as to lessen opponents' ability to perform various kinds of packet forwarding malpractice.

[24] surveyed the WSN application in environmental monitoring, employing specific water quality importance. A variety of WSN dependent methods for water quality monitoring that were recommended by other authors was analyzed and studied because of their energy, coverage, and security aspects.

[25] presented a view on WSN, which has been engaged previously in many areas like industry, health, and military. With several intrinsic restrictions in WSN, a critical concern is a security. The stated functions of the wireless network security must be well established. In this, a technique of security challenging depends on security levels wererecommended for WSN. The investigationalresultsexpose that the platform was the most possible one for the security level assessment module in WSN.

[26] allowed the reliable data transmission while malicious attacks happen in the network. Trust based data transmission done through three approaches that are: initially, trust-based data packets prediction, secondly, Trust based recommendation calculation and computes the integration of direct trust evaluation between the nodes.[27] considered a system of phishing detection, which can detect this kind of attack using some machine learning algorithms and recognition of some visual similarity employing some natural language processing techniques aid. Many tests have been applied to the proposed system, and experimental consequences showed that algorithm Random Forest has a very better performance with a 97.2%success rate.

[28] Proposed the LEACH protocol for the community creation and the exchanging of confidence values between member Nodes, master Nodes and Base Station.

[29] presented a work which focuses on Cloud integrity and privacy mechanisms that will rely on hardware tamper-proof and cryptographic data structures that were energy-efficient and proves to be a suitable one for the un trusted Cloud environments process. The wormhole attack is feasible though the assailant did not conciliation

the host, despite the circumstance that communication entirely bids authenticity and confidentiality. In the attack wormhole, this deteriorates the performance gain of network coding. Projected a method that was not in favor of sinkhole attacks and identifies malicious nodes with the use of hop counting. The major benefit of the projected method was that a node was capable of identifying malicious nodes in collaboration with neighbor nodes devoid of requiring any concession with BS (base station). False detection of attacks was the major limitation of this wok.

3. Proposed Work

The proposed flow focuses mostly on the detection of data link breaks and the determination of shortest path with the use of implementedstructure. The figure 2signifies the entire shortcut illustration of the projected work-flow.

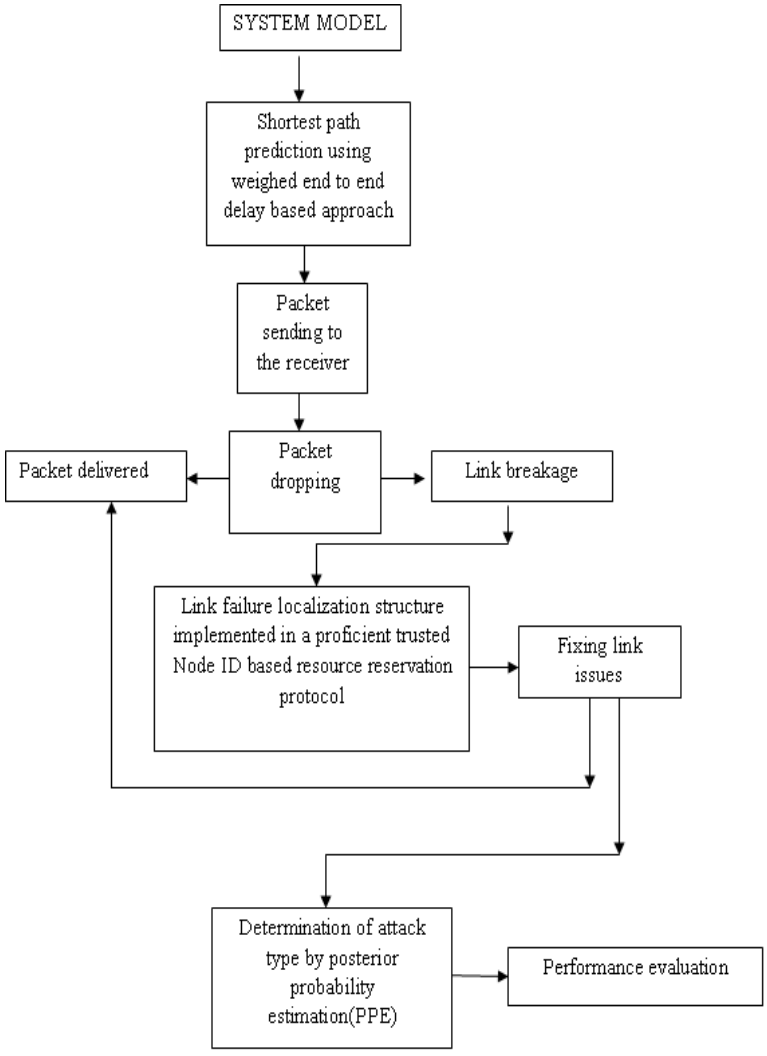

Figure 2 Schematic representation of proposed methodology

A. ***System model and Node initialization***

Initially, two general models were presented to give a suggestion regarding the transformation of information among sensor nodes. It was assumed that there was N number of sensor nodes that were moving at some distance as per the reference region model of group communication. The entire nodes in the model have the equivalent range of transmission. Each node is capable of transferring information to the neighboring nodes. Initially, here the hop, nodes and the channel can be initialized. A field of interest occurs for any data point. In this field, data should be maintained (some nodes in this region should be established). Information and details are transmitted down to the region concerned by the source node. Selecting the node can be defined as a problem that can be represented as**,**

$$D_{cn}=\sum_{l=1}^{l=m-1} OP(s_l, s_{l+1}) \frac{1}{m}.(m-1)\text{C} \qquad (1)$$

Where s_l is the node for the data carrier, C is the channel, l is the number of data carrier nodes used by the entire time domain, and OP (s_l, s_l +1) is the network link between s_l and s_l +1. The data in the network is S, and the contact time between s_l and s_l+1 is OP (s_l, s_l+1). D here is the distance from $s_l$to the center area of interest. M is the number of nodes. First, consideration must be provided to latency between the current data carrier node and the adjacent node, as low-throwing links that increase channel time required for data transmission.

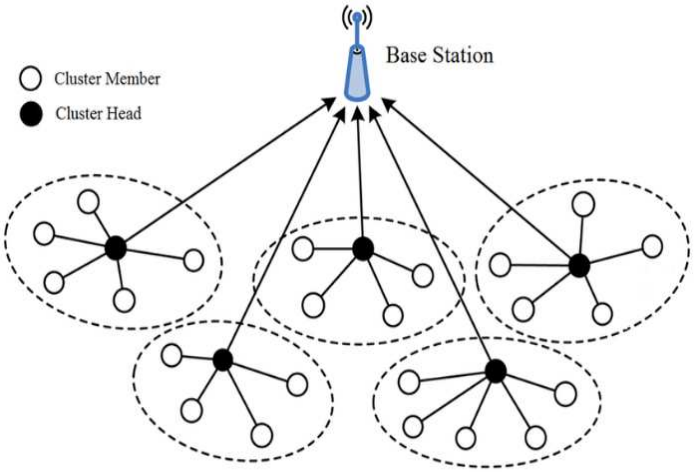

Figure 3 system model and node deployment in WSN

In this, the nodes are capable of communicating with one another by multi-hop systemformation. The packets of data could be sent through the source and thus thisshouldreach the destination node over several jumps or skips. The process of communication might be regarded as successful only when there might be good co-ordination between the nodes. Initially, there wasquite a lot of nodes numbers wereheremainly they want to cluster henceforth the systembecomes separated into the sub-structures which are interconnected afterward the group will bemade. There was a cluster head in each formed cluster. A base station role can be played by each leader in the group or cluster.

Each sensor is initialized with the consideration for numerous limits that comprise residual battery power, network connectivity, security, reliability, network lifetime, and link lifetime for choosing the most favorable Cluster Heads (CH). Here, to initialize the sensor nodes across the source node to the destination node according to

inter- cluster topology and intra-cluster topology with optimum throughput, packet delivery ration, and energy consumption etc. The normal nodes and the cluster head selection.

The main purpose of theclustering is to sustain the systemof keyadministers and management of acluster mostly. This kind of grouping mightdecrease the keys primarily intended for the communication processpurpose. The entire packetinformation can influence the cluster head beforehand it influences the source ofdestination. The clustering process might be done for enhancing thesecurityof networkand also to sustain the proper process ofcommunication**.**

B.*Prediction of shortest route or path by means of weighted based end-to-end approach:*

In the prevailing approaches the data could be sent from source to nodeof destination. Just if there might be the occurrence of malicious node revenue the method becomesbreaks and formerlythis wouldbe originated to the source node once more and formerly it will resume the procedure. Originally, it won't distinguish where must be the linkage breaking is existing henceforth if it starts the process once more then there might be time and energy wastage. Therefore, there will be a necessitate to overwhelm issues through implementing the approach of weighted based end-to-end delay. This methodgoal was to aim the node of destination in the initial attempt de-void of wasting energy and time. The weighed based delay approach is employed for estimating the shortest routeamong nodes. The interruption was then affected by means of hops number at which the packets need to pass through. The length of hop amongdestination and source changes corresponding to the time. In this, the protocol employed is the PTN-RRP protocol. This routing etiquette was introduced aimed at the specified net-work deployment.

The packet delay was proportional to the path lengthdirectly. In case, the path length increases then the delay becomes increased. In this, there might be simple relation among the delay of packet and thepath length. In the presented weighted delay, the shortest route is being estimated on recognizing the path's weightage length among the nodes from source. The weighted route is regarded as the path having small distance and in turn lacks the breakage of link. Following the route estimation, the information packets will be sent directly to the nodeof destination. This is a time validprocedure somewhat that saves the energy too.

Algorithm: selection of shortest path by means of weighted based end-to-end delay technique

---

Procedure: prediction of the shortest path

Inputs: Hops and Sequence number

Outcome: the shortest route from source node to destination node

Stage1: the parameters of hop are initialized like a communication range and the nodes number

Stage2: the negligible hop count data/information is attained among respective node

Stage3: Estimate the distance among sensor nodes in an average

Stage4: Evaluate the distance assessed among the nodes

Stage5: Assessment of locations of node

Just the calculation of distance among every node there is a an necessitate for search in the link breakage among nodes. As there is breakage in link the packet information might originate to source and a process is regained. Therefore, the breakage of link finding is introduced and the PTN-RRP was established for link breakage estimation easily.

C.*Link failure localization structure implemented in a PTN-RRP protocol*

A PTN-RRP protocol might not offer any services in the network. The etiquette having characteristics of traffic among the sensor nodes will be explained clearly. The path messages are sent todestination from source. In this, the messages were transmitted by means of various hops. Each node in this was determined by their respective Id's. this protocol is the one at which the nodes are estimated whether it is necessary or not. The common messages or information's will be employed for monitoring and detecting links with neighbors. In case, the common messages were used, every node that is active will transfer common message periodically to the complete node. In case, the node doesn't receive any normal information from neighbor then the link gap is predicted. This employs the simplex flows generally over the network. The message route comprises the information regarding sources that is needed for the purpose of connection. The reservation process can begin though the path message grasps the router. Formerly the incoming router directs the reservation message towards the outbound handler. Afterwards getting the message, the incominghandlerfounds additional unidirectional route. Till the session was active the route can simply open. Now, the quality of the service was certain in addition to the bandwidth guaranteed. It provided the assurance on the packets then it does not deliver assurance in the interruption difference. Mostly the nodes ID here couldshowasignificantpart in this procedure be subject to the id node it couldrestrict the node thenrecognizelinkage break.

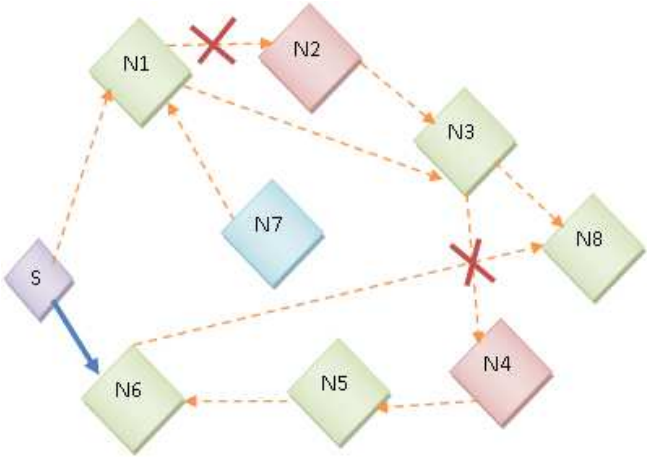

Figure 4 link breakage duringtransfer of data

The figure 4signifiesprojected technique of short route detection that lacks the link breakage. At this time that the scenario above was assumed at which the source node is an N2starting fact and is N4malicious node and is the cluster head N7 and is the destination nodeN6. In this, there is connectionamongthe entire sensor nodes. Through the PTN-RRP protocolimplementation withapproach weighed end to end delay after the method of the investigation can be madeafterwardswhich could be summarized that for N6 destination, the subjective route was recognized and the data could permit in a first attempt successfully. Typically, this in turn will save energy and time.

As the link failure monitoring conditions are satisfied, and then the process of route establishment takes place, which in turn maintains the better path for communication. The QoS based performance analysis is carried out to ensure better transmission of data among the nodes without any link failure.

D. ***Attack determination using posterior probability estimation (PPE)***

The WSN wasjust an open package which will subjects to various attack types. For the attack determination, the method of posterior probability assessment is employed. This is one such posterior probability distribution technique employed for determining the values prediction that are unknown and the scheme will be based on the selection of random variables. The major intention was that it could search for background that are relevant and in turn observes the data that are relevant. So as to attain this intention, it is essential to offer regular interval. Typically, this could perceive the probability of member and could uncertainly reflect the values.

Let us consider the variable's probability distribution that could be estimated with the use of Bayes theorem. This will be computed on multiplying the values of probability distribution and after that attaining vale by dividing the normalizing constant.

$P(\emptyset/x) = (p\frac{(\frac{x}{\emptyset})}{p(x)})P(\emptyset)$(2)

Where, $P(\emptyset) is\ the\ function\ of\ probability\ distribution$,

$P(\frac{x}{\emptyset})$ is the functionof likelihood

$P(\emptyset/x)$ is the functionof evidence

The posterior likelihood might be in the posterior probability form which is proportional to the probability directlywhich is a prior multiplication of probability.

$F(x) = [f(x)\ L(x/y=y(x)/\int_{-\infty}^{\infty} f(x)(u)L(x/y = y(x)(u)du]$ (3)

Where,

F(x) is the functionof preceding density

f(x) L(x/y=y(x)

which is a functionof likelihood

$f(x)(u)L(x/y = y(x)(u)$,

which is a normalizing constant.

i. Posterior probability calculation

The fundamental transition probability expression is as given below:

$$Tp_{ab}(t) = \frac{\tau_{ab}^{\beta} g\eta_{ab}^{\beta}(T)}{\sum_{L\in n_a} \tau_{aL}^{\beta} g\eta_{aL}^{\alpha}(T)} \text{ , if } b\in n_a \quad (4)$$

$$0, \text{ if } b\neq n_a$$

The greatest pheromone value is the superior the link quality influence on the selection of packet path in the network. In the transmit pheromone probability formula, the importance is on posterior probability. The additional weight features can be place according to the diverse situations via observed values or simulation study. When the swarm finishes a routing or chooses the next hop routing, or the cycle set updation by the routing protocol appears, the selected path's pheromone probability is revised according to the given formula:

$$\tau_{ab}(T+1) = (1\text{-}\rho)\ \tau_{ab}(T) + \rho\Delta\tau_{ab}(T) \qquad (5)$$

Where, $\tau_{ab}(T)$ is amount of pheromone on the link (a, b)

ρ is the evaporation time of the pheromone

The ρ value range is $\rho \in [0,1]$. So, $1 - \rho$ describes the pheromone's enduring level.

ii. Degree assignment

Here, the neighborhood hop prediction establish through the degree assignment method. The degree of a node refers the number of sensor nodes in the neighborhood of the sensor node. The degree assignment establishes the route overhead reduction with optimal design consideration. The number of message exchanges required is a function of degree of nodes in the network. Depends on the pheromone probability values, the prediction is enabled. The hop count of the network was increased by 1 during the degree assignment. Here, the MPR-link optimized routing protocol provides the well-known neighborhood sensor nodes. The prediction of neighborhood hop furnishes the link quality, without link failure etc. in the network.

iii. Link quality estimator

Link quality estimation is the major concerns for running in wireless Networks and emerging Unmanned System networks-based applications. Link quality estimator is a noteworthy issue that disturbs rates of sensor nodes transmission and metrics of link quality that were employed to assess a quality of link. MPR-based optimized routing protocols frequently rely on link quality evaluations to choose consistent data links and sustain proficient network function. Though the lossy and the energetic performance of the data links creates this non trivial task. To acclimatize the link quality estimation among the reliable sensor nodes according to the link solidity, a dedicated algorithm supervises the window size growth after its attack's reduction. Then, the window Size (WS) is enhanced or transferred (the window is transferred left) below the given conditions:

$$\mathrm{WS} = \begin{cases} enhanced & WSn \geq Th \cap Cn \geq \frac{WS_n}{2} \\ transferred & else \end{cases} \qquad (6)$$

After every increased link quality, the counter C_n is reset. The link quality approach limits the window size speed according to the loss incidence and regulates the accuracy of the link quality estimation in the sensor node networks according to the link stability.

Essentially, the probability function was to chart out the function of likelihood. Formerly after recognizing the prior likelihood the attack will be identified.

4. Performance Analysis

This section is the deliberation of performance analysis of the proposed mechanism. The performance evalua-

tion of the proposed methodology gets explained in this section. The comparative analysis offered with existing techniques [30]to establish the effectiveness of proposed mechanism. The experimental analysis simulated using MATLAB.

1. Packet delivery ratio

Collectively, this refers to the number of packets that are transferable by the sender received by the recipient.

$$P = (Pr / Ps) *100 \quad (7)$$

P is the transmission ratio of the packet; PR is the sum of packets obtained and Ps the volume of packets forwarded.

2. False positive rate (FPR)

The false positive rate or incorrect rate of incidence is measured as a combination between the number of incorrectly classified negative events and the overall number of negative events.

$$\text{False positive rate} = FP/(FP+TN) \quad (8)$$

Table 1 represents the average packet delivery ratio comparison of the proposed system (PPE-IDS) with the existing techniques employed for IDS. The comparison is estimated in terms of number of nodes. The proposed system offers better outcome than the existing techniques. Thus, this analysis shows the effectiveness of proposed strategy.

Table 1 Average Packet delivery ratio

No of nodes	NNTB-IDS	EATB-IDS	TE-IDS	PPE-IDS (Proposed)
10	0.9	0.92	0.95	0.98
20	0.85	0.88	0.93	0.964
30	0.79	0.85	0.9	0.933
40	0.73	0.8	0.865	0.89
50	0.645	0.79	0.81	0.85

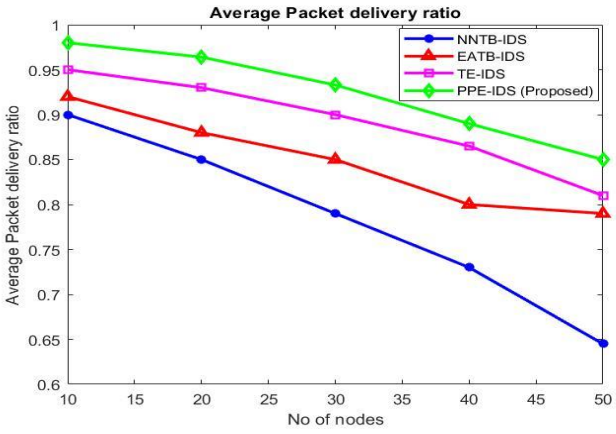

Figure 5 Average packet delivery ratio comparisons

Figure 5 is the graphical representation of the proposed system (PPE-IDS) and existing techniques comparison made in terms of average packet delivery ratio. The average packet delivery ratio is higher than the existing techniques. Thus, the proposed scheme is effective in delivering high rate of packets to the destination node.

The detection ratio or the rate of prediction is estimated to prove the effectiveness of proposed protocol performance for detecting link breakage. The detection ratio is carried out to estimate the link breaks occurred during transmission of data. Table 2 signifies the ratio of detection comparison made for proposed and existing techniques. The analysis shows that the proposed method offers better DR than the existing techniques.

Table 2 Detection ratio (DR)

No of nodes	PTN-RRP(proposed)	WT-MND	WTE	WTE(R)	WTA
100	0.998	0.994	0.894	0.993	0.991
200	0.993	0.989	0.979	0.989	0.978
300	0.991	0.987	0.963	0.982	0.979
400	0.990	0.991	0.958	0.984	0.983
500	0.989	0.986	0.957	0.982	0.974
600	0.980	0.982	0.953	0.974	0.961
700	0.985	0.984	0.941	0.972	0.953
800	0.992	0.988	0.958	0.967	0.938
900	0.990	0.983	0.959	0.963	0.926

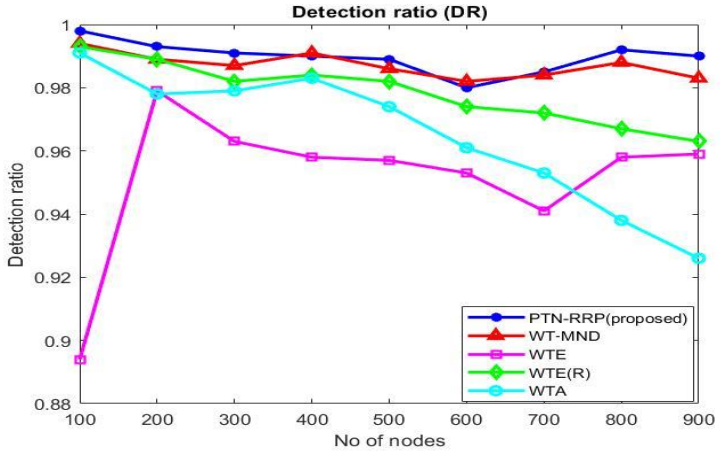

Figure 6 comparative analysis of DR

The graphical representation of detection ratio comparison is provided in figure 6. The detection ratio is estimated by varying the number of nodes which ranges from 100 to 900 nodes. The proposed PTN-RRP protocol is analyzed to be effective than the existing protocols employed for link breakage detection. Thus, the detection ratio of proposed protocol is higher and varies as per the number of nodes.

Table 3 indicates the ratio of malicious detection ratio (MDR) comparison made for proposed and existing techniques. The analysis shows that the proposed method offers better MDR than the existing techniques. It is estimated for the purpose of detecting malicious or fake prediction. The ratio is estimated by varying the number of nodes that ranges from 100 to 900 nodes. From the analysis it was evident that the proposed strategy is better than existing ones.

Table 3 Malicious Detection ratio (MDR)

No of nodes	PTN-RRP(proposed)	WT-MND	WTE	WTE(R)	WTA
100	0.009	0.012	0.797	0.143	0.016
200	0.012	0.018	0.783	0.231	0.062
300	0.024	0.026	0.779	0.208	0.055
400	0.022	0.028	0.775	0.202	0.047
500	0.020	0.021	0.775	0.198	0.058
600	0.026	0.032	0.775	0.195	0.083
700	0.029	0.037	0.794	0.271	0.093
800	0.032	0.035	0.812	0.236	0.098
900	0.027	0.031	0.827	0.261	0.104

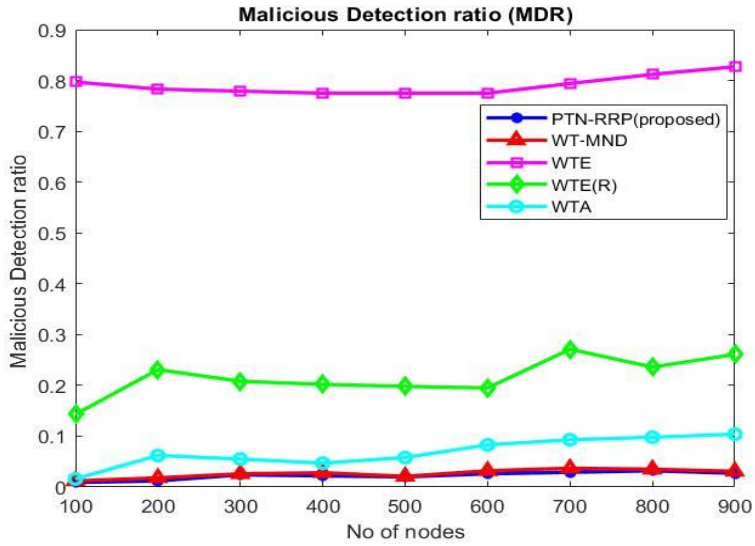

Figure 7 comparative analysis of DR

The malicious detection ratio comparison is provided in figure 7as a graphical illustration. The malicious detection ratio is estimated by varying the number of nodes that varies from 100 to 900 nodes. The PTN-RRP proposed protocol is examined to be lower than the existing protocols employed for link breakage detection. Thus, the detection ratio of proposed protocol is lower and varies as per the number of nodes.

Table 4 denotes the SD comparison between DR and MDR for the proposed system (PTN-RRP) protocol with the existing techniques. The proposed system offers lower SD range than the existing techniques. Therefore, this analysis shows the effectiveness of proposed protocol.

Table 4 Standard deviation for DR and MDR comparison

Methods	DR standard deviation	MDR standard deviation
PTN-RRP(proposed)	0.002952	0.007013
WT-MND	0.003887	0.008276
WTE	0.023659	0.018566
WTE(R)	0.010064	0.032964

WTA	0.021953	0.028492

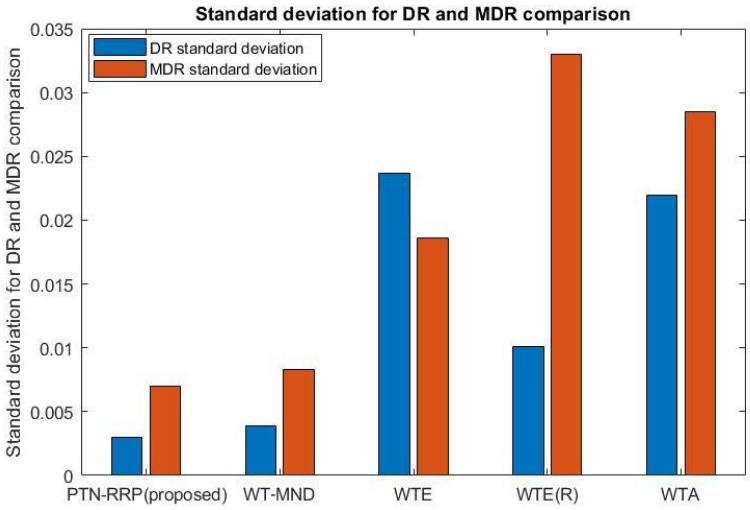

Figure 8 comparative analysis of Standard deviation for DR and MDR

Figure 8 is the graphical depiction of the proposed system (PTN-RRP) and existing techniques comparison made in terms of SD among DR and MDR. The SD is lower than the existing techniques. Thus, the proposed scheme is effective in offering better SD for both DR and MDR.

Table 5 signifies the analysis of False positive rate (FPR) comparison made for existing and proposed techniquePPE-IDS. The investigation illustrates that the projected technique offers lowerFPR than the existing techniques.

Table 5 analysis of False Positive Rate

No of nodes	**NNTB-IDS**	**EATB-IDS**	**TE-IDS**	**PPE-IDS (Proposed)**
10	0.049	0.048	0.047	0.045
20	0.052	0.05	0.049	0.047
30	0.1	0.053	0.051	0.049
40	0.155	0.12	0.055	0.052
50	0.34	0.19	0.125	0.058

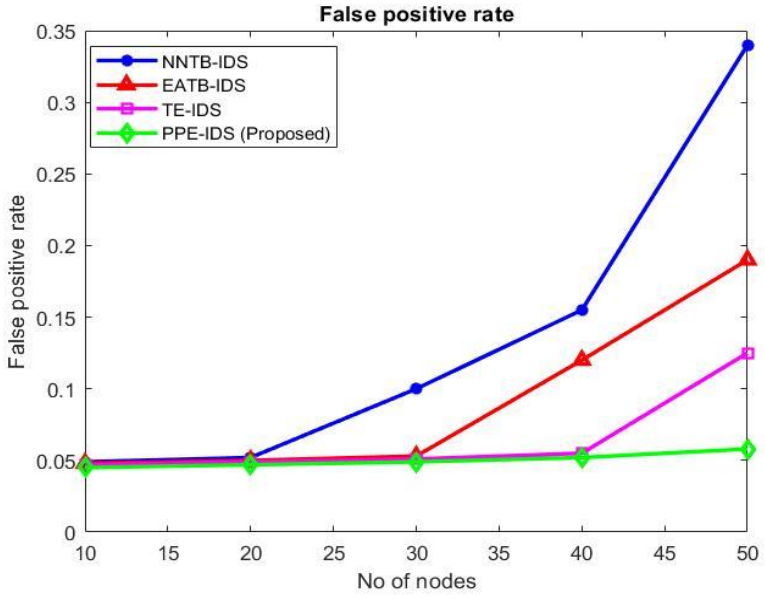

Figure 9 comparative analysis of False Positive Rate

Figure 9 is the graphical illustration of the proposed system (PPE-IDS) and existing techniques comparison made in terms of FPR. The FPR is lower than the existing techniques. Thus, the proposed scheme is effective in offering lower rate of false positives. Therefore, the performance and comparative analysis shows that both proposed protocol PTN-RRP for link breakage detection and the PPE-IDS scheme for attack detection is better than the other existing strategies.

5. Conclusion

The breakage of link in the route will lead to the rise in the packet loss amount in the network. Henceforth, because of this QoS will somewhat decreased and is a challenging problem. So as to overcome the issues, the proposed protocol (PTN-RRP) was introduced along with the scheme of average weighted based end-to-end delay method. The mechanism of link breakage was incorporated in this protocol to maintain route in an effective manner. In this, the nodes receive data packets and in turn checks that the breakage of link is existing or not elsewise the link might go to interruption means afterwardstochoosealternative path. These progressions canendure till it can attain the short and path which is link break absence. After that, the correct route getting can send the packets data to the destination node in one attempt. After that the posterior probability evaluation method was implemented to predict the cause of link failure if whether it due to any kind of the attack means the probability method can predicts the type of the attack very easily. The performance simulation is carried out in terms of accuracy, throughput, delay, PDR, no of link breakage, and overhead to prove the effectiveness of proposed strategy.

Conflict of interest:
There is no conflict of interest.
Funding:
There is no funding information.

Availability of data and material:
There is no availability of data and material.
Code availability:
There is no code availability.
Author's contribution:
There is no author's contribution.

REFERENCES

[1] Y. Chittibabu, C. Anuradha, and S. R. C. P. Murty, "Fuzzy Trust Based Energy Aware Multipath Secure Data Collection in Wireless Sensor Network," *Journal of Computational and Theoretical Nanoscience,* vol. 16, pp. 669-675, 2019.

[2] S. Jaggi and E. V. Wasson, "Enhanced OLSR Routing Protocol Using Link-Break Prediction Mechanism for WSN," *Industrial Engineering and Management Systems,* vol. 15, pp. 259-267, 2016.

[3] R. Gunavathi, "Improved Trust based Variants of AODV Routing Protocol for Wireless Sensor Networks."

[4] A. Ahmed, U. Ashraf, F. Tunio, K. A. Bakar, and M. S. AL-Zahrani, "Stealth jamming attack in WSNS: Effects and countermeasure," *IEEE Sensors Journal,* vol. 18, pp. 7106-7113, 2018.

[5] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang, "Enabling security functions with SDN: A feasibility study," *Computer Networks,* vol. 85, pp. 19-35, 2015.

[6] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," *Wireless Personal Communications,* vol. 110, pp. 1637-1658, 2020.

[7] D. Nehra, K. S. Dhindsa, and B. Bhushan, "A Security Model to Make Communication Secure in Cluster-Based MANETs," in *Data Engineering and Communication Technology*, ed: Springer, 2020, pp. 183-193.

[8] P. Sherubha, P. Amudhavalli, and S. Sasirekha, "Clone attack detection using random forest and multi objective cuckoo search classification," in *2019 International Conference on Communication and Signal Processing (ICCSP)*, 2019, pp. 0450-0454.

[9] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy*, et al.*, "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access,* vol. 8, pp. 65450-65461, 2020.

[10] C. Sasikala and A. Senthilkumar, "Secure disjoined multi-hop communication in wireless sensor network using trust nodes based data transmission technique," *Materials Today: Proceedings,* 2021.

[11] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access,* vol. 7, pp. 79980-79988, 2019.

[12] P. A. Patil, R. S. Deshpande, and P. B. Mane, "Trust and Opportunity Based Routing Framework in Wireless Sensor Network Using Hybrid Optimization Algorithm," *Wireless Personal Communications,* vol.

115, pp. 415-437, 2020.

[13] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Computers & Electrical Engineering,* vol. 66, pp. 274-287, 2018.

[14] U. S. R. K. Dhamodharan and R. Vayanaperumal, "Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method," *The Scientific World Journal,* vol. 2015, 2015.

[15] M. I. Abdullah, M. M. Rahman, and M. C. Roy, "Detecting sinkhole attacks in wireless sensor network using hop count," *Int. J. Comput. Netw. Inf. Secur,* vol. 3, pp. 50-56, 2015.

[16] A. Rajeswari, K. Kulothungan, S. Ganapathy, A. J. P.-t.-P. N. Kannan, and Applications, "A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks," vol. 12, pp. 1076-1096, 2019.

[17] R. Kumar and S. Shekhar, "Trust-Based Fuzzy Bat Optimization Algorithm for Attack Detection in Manet," in *Smart Innovations in Communication and Computational Sciences*, ed: Springer, pp. 3-12.

[18] N. Dharini, R. Balakrishnan, and A. P. Renold, "Distributed detection of flooding and gray hole attacks in Wireless Sensor Network," in *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 2015, pp. 178-184.

[19] Q. Zhang and J. Xiao, "Improve security of wireless sensor networks through reluctant checksum," *International Journal of Distributed Sensor Networks,* vol. 13, p. 1550147717731041, 2017.

[20] O. Adarkar, R. Mane, and D. Shah, "IMPACT OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK," 2018.

[21] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in *Proceedings of the World Congress on Engineering*, 2015.

[22] M. Naik and N. Geethanjali, "A Multi-Fusion Pattern Matching Algorithm for Signature-Based Network Intrusion Detection System," 2016.

[23] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET," *SpringerPlus,* vol. 5, p. 995, 2016.

[24] M. Pule, A. Yahya, and J. Chuma, "Wireless sensor networks: A survey on monitoring water quality," *Journal of applied research and technology,* vol. 15, pp. 562-570, 2017.

[25] M. Wei and K. Kim, "An automatic test platform to verify the security functions for secure WIA-PA wireless sensor networks," *International Journal of Distributed Sensor Networks,* vol. 12, p. 1550147716676094, 2016.

[26] D.-g. Zhang, J.-x. Gao, X.-h. Liu, T. Zhang, and D.-x. Zhao, "Novel approach of distributed & adaptive trust metrics for MANET," *Wireless Networks,* vol. 25, pp. 3587-3603, 2019.

[27] E. Buber, B. Diri, and O. K. Sahingoz, "NLP based phishing attack detection from URLs," in *International Conference on Intelligent Systems Design and Applications*, 2017, pp. 608-618.

[28] S. Ramesh and C. Yaashuwanth, "Enhanced approach using trust based decision making for secured wireless streaming video sensor networks," *Multimedia Tools and Applications,* pp. 1-20, 2019.

[29] W. Itani, A. Kayssi, and A. Chehab, "Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing," in *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, ed: IGI Global, 2019, pp. 731-763.

[30] F. Zawaideh and M. Salamah, "An efficient weighted trust-based malicious node detection scheme for wireless sensor networks," *International Journal of Communication Systems,* vol. 32, p. e3878, 2019.