International Journal of Digital Crime and Forensics
Volume 13 • Issue 5 • September-October 2021

Malevolent Node Detection Based on Network Parameters Mining in Wireless Sensor Networks

Sunitha R., PES University, Bengaluru, India
Chandrika J., Malnad College of Engineering, Kamataka, India

ABSTRACT

The exponential growth of the internet of things and united applications have renewed the scholarly world to grow progressively proficient routing strategies. Quality of service (QoS) and reduced power consumption are the major requirements for effective data transmission. The larger part of the applications nowadays including internet of things (IoT) communication request power effective and QoS-driven WSN configuration. In this paper, an exceptionally strong and effective evolutionary computing allied WSN routing convention is designed for QoS and power effectiveness. The proposed routing convention includes proficient capacity called network condition-based malicious node detection. It adventures or mines the dynamic node/network parameters to recognize malignant nodes. Experimentation is done using network simulator tool NS2. Results ensure that the proposed routing model accomplishes higher throughput, low energy utilization, and low delay that sustains its suitability for real-time WSN.

KEYWORDS

Bayesian Network, IEEE 802.15.4 MAC, Malevolent Node, Network Mining, Quality of Service, Queuing Overflow, Wireless Sensor Network

1. INTRODUCTION

The exponentially swift in wireless communication systems and associated applications have revitalize the research-industry to develop progressively capable and strong routing technique to fulfil growing demands. Contemporarily, the modern era of human lifestyle cannot be assumed without having communication system where each known and unknown intelligence will be utilized by every user to share information among multiple peers by making optimistic decision. There exist many applications include wireless sensor network components are military, Healthcare, Smart industries, spatio-temporal, smart agricultural, smart home, SCADA, smart city, etc (Azlan & Al-Anbuky, 2015; Ehsan & Hamdaoui, 2012; Medeiros de Ara'ujo & Becker, 2011; Spachos et al., 2015). On the other hand, to increase the QoS communication requirement by providing timely, reliable, and power efficient communication among the several deployed nodes in the network area as there is a demand for significant development of network computing and dynamic decision-making applications. Machine-to-Machine (M2M) communication and Internet-of-Things (IoT) are two among the recently developed technologies which apply wireless communication protocols as a backbone network to provide real-time data transmission among nodes to provide ideal energetic decision making

DOI: 10.4018/IJDCF.20210901.oa8

(Ehsan & Hamdaoui, 2012). Its significances have expanded towards Big Data analytics, Industrial Interaction, Monitoring and Controlling, Enhanced Surveillance functions and so forth. To fulfill above stated requirements, distinctive network prototypes have been proposed, among which WSN is the overwhelming one.

WSN being a decentralized and infrastructure-less communication paradigm includes various sensor nodes distributed over the network that work agreeably to transmit detected data from source to the sink node in one or many hops. However, dynamic nature of the network and the node situations regularly impacts transmission effectively, compelling WSN to experience connection-outage, congestion, packet drop and retransmission (Medeiros de Ara'ujo & Becker, 2011). Such challenges frequently result into more energy-dissipation causing network life-time degradation and QoS violence. On the other hand, Quality of Service and Quality of Experience (QoE) being the unavoidable requests of the traditional communication frameworks require WSN to guarantee ideal information transmission over the network. Along with QoS provision, WSN being battery operated network needs ideal routing mechanism to reduce packet loss and retransmission probability and the sub-sequent node death rate to hold maximum network lifetime (Ehsan & Hamdaoui, 2012)(Medeiros de Ara'ujo & Becker, 2011)(Sen & Ukil, 2009). Sensor nodes are very sensitive to the vulnerabilities and often deployed in some dangerous environments. These nodes can get failure due to the hardware problem of any damages or by draining the energy. In the wireless networks, the node failure will be more than one normally compared to the wired or infrastructure-based wireless network. There is a need for the routing protocol deployment which detects the failures as early as possible and efficient enough to handle a greater number of faults meanwhile managing all the network functionalities. So, the routing protocol should automatically select the alternate paths if there is a node or link failure in one path.

In traditional WSN either static network parameters are utilized for routing decisions or particular security models are used to recognize malevolent nodes to maintain a strategic distance from their quality in transmission path. In any case, these techniques as an independent solution cannot ensure optimal performance, particularly under dynamic network conditions and intelligent malevolent node presence. In the majority of the existing WSN routing protocols, authors have applied node parameters such as residual energy, packet drop per node, link quality, congestion probability, etc. to perform routing decisions. Interestingly, authors have used a single network condition parameter to make routing decisions. However, in contemporary network scenarios the presence of dynamic nodes and/or network conditions cannot be ignored, which eventually could influence the efficiency of the routing protocol. On the other hand, even a malevolent node can also impact overall network performance. Malevolent nodes can have sufficient (resembling) node parameters mimicking the genuine nodes, whose inclusion in the forwarding path can lead to packet drop, energy exhaustion, delay, loss of data, etc. Hence, in addition to the network condition aware routing decision, malevolent node identification and avoidance is a must to ensure QoS provision in wireless sensor networks. To achieve this, network mining concept can be vital where exploring different nodes as well as network parameters over the operating period can helps in identifying malevolent nodes to avoid it and making an optimal adaptive routing decision.

The remaining sections of the presented manuscript are divided as follows: Section II discusses related work, which is followed by research questions and problem formulation in Section III. Overall proposed system and its implementation is discussing in Section IV. Section V presents the simulation results and allied inferences, while overall conclusion is given in Section VI. References used in this research are given at the end of the manuscript.

2. BACKGROUND

This part of the paper basically talks about some of the key writings pertaining to the focused research target of designing powerful anomaly identification mechanism for WSNs. Prominently,

the above-stated objective has been achieved in most of the existing approaches. Contrasting with these existing approaches we concentrate on the different network parameters on designing an ideal cohesive resolution to accomplish QoS as well as energy-efficiency requirements. Zhang et al (2019) concentrated on exploiting node validity and time-series analysis to be applied in urban network circumstances by identifying anomalies for improved routing decisions in dense WSN. Authors have implemented a Bayesian model to attain the status value for every partaking node which has been contrasted with a pre-defined threshold range to identify a node as malevolent or intruder. They are not concentrating on the delivery ratio and security tradeoffs in the network.

Kumar et al (2018) implemented a Bayesian Network model to calculate the conditional dependency among the participating nodes in the network to detect malevolent nodes. This system is not considering the dynamic nature of the wireless sensor network, it works efficiently for the static sensor network. Xu et al (2012) developed a combined support vector machine and K-Nearest neighbor (SVM-KNN) based approach to detect Malevolent in a wireless sensor network. The authors implemented KNN to get statistics among the adjacent nodes of the network, and SVM was used as a spatial-temporal classifier to identify the malevolent or outlier node. The authors also suggested that there exist other techniques that can reduce the data samples to detect the outliers still accurately.

Martins et al (2015) designed a multi-agent model for outlier detection in WSN. To accomplish it, the authors used the Least Squares SVM model to learn dynamic time-series network data to identify outlier nodes. Here authors designed a multi-agent hierarchical structure and the node if it is not an agent and if it is an outlier then it will not be detected properly. Liu et al (2013) designed an adaptive routing protocol based on knowledge-driven training, in this approach at first minimization concept was used to detect Malevolent, followed by this link-level context-aware rate adaptation model for making routing decisions is also designed. By this model overall 18% throughput was achieved. Erroneous data in the context information will be identified as an outlier.

Feng et al (2017) considered node's credibility feedback to identify distributed malicious node in WSN. Authors used Bayesian-based reliability calculation to perform malicious node detection, it is good for traditional networks but too complex and suspicious for the dynamic network. Zhang et al (2010) developed an approach by considering network surveillance, unique message or fake message detection, and various spatial-temporal association and consistency. Here authors considered multiple parameters to identify malicious data.

Yessembayev et al (2018) too worked on distinguishing WSN nodes as good or bad based on altered or unreliable information transmitted by a malicious node. Here authors are not monitoring detected nodes in the network, and they mentioned a suggestion for concentrating on the reliability of the network to maintain after the bad node detection in the network. Abid et al (2017) applied a density-based spatial clustering approach for malicious node detection. And clustering is not only enough to provide more quality of services in the wireless sensor network. Paola et al (2015) developed an adaptive distributed Bayesian model for Outlier detection in WSN. The authors are concentrating on the data outliers and it is not sufficient for the optimal routing and to increase the energy efficiency. Rajasegarar et al (2010) developed centered Hyper-spherical and Hyper-ellipsoidal One-Class SVM for malicious node detection in a sensor network. The authors developed a one-class quarter-sphere SVM (QSSVM) that retrieves normal data vectors in a higher dimensional space for each participating node to perform anomaly detection. This model may be inefficient for the dynamic behavior of the sensor networks because the authors suggested enhancing it for different parameter adjustments.

Yang et al (2019) developed a graph rigidity concept for malicious node detection ad localization in WSN. Here, the authors applied inter-node distance information to perform malicious node detection; however, its efficacy for mobile-WSN seems to be limited. Recently, Zhang et al (2010) applied an artificial neural network algorithm to perform malicious node detection in WSN. This approach considers the temperature reading provided by a node to assess its reliability. However, its efficacy remains confined to smart home (indoor) purposes only. Wang et al (2016) developed an isolation-based outlier detection approach using nearest neighbor ensembles (iNNE). Their approach

exploited Spatio-temporal information obtained by nodes to perform outlier identification. Ghorbel et al (2018) developed a kernel principal component analysis (KPCA) to classify data as normal or malicious. The authors applied the KPCA-based Mahalanobis kernel to detect Malevolent in a sensor network. this work is concentrating on the identification of outliers in the training data and not suitable for more energy efficiency of the nodes.

For a selective forwarding attack, a malicious node detection algorithm based on a triangle module fusion operator (MDTMO) (Yessembayev, 2018) is suggested. After the base station node receives the warning information, the monitoring node will then alert the base station node, further verifying whether the packet loss is caused by network congestion or attack. If the network quality is good and there is no congestion, the node is described as a selective forwarding attack launched by a malicious node. Then the base station node sends an alert message, and the network isolates the malicious node.

A systematic literature review of current clone node identification schemes was proposed by Muhammad Numan et al (2020). In the remote and harsh environment, the deployment of WSNs enables the opponent to capture the valid node and collect stored credential information such as IDs that can be easily re-programmed and reproduced. This is the primary inspiration for researchers to design improved clone attack detection protocols. We have thus presented a systematic literature review of current clone node detection schemes in this paper.

The deep neural network (DNN) developed by Swarna Priya R M et al (2020) is used to build efficient and appropriate IDS in the IoMT setting to identify and anticipate unforeseen cyberattacks. The network element is preprocessed by hyperparameter selection methods, optimised and tuned. The benchmark intrusion detection dataset compares a detailed study of DNN experiments with several other machine learning algorithms. Moutaz Alazab et al (2020) designed an efficient classification model that combines permission requests and API calls. As many APIs are used by Android users, we suggest three distinct grouping strategies to pick the most useful API calls to increase the probability of Android malware apps being identified: the uncertain group, the dangerous group, and the destructive group. The findings indicate that malicious applications invoke a different collection of API calls compared to benign apps and that mobile malware frequently demands hazardous permissions more often than benign apps to access sensitive data.

In the existing methods, there are a lot of shortcomings like malicious node detected may be kept idle for some time then it can be removed from the network, energy consumption is more in identifying malicious nodes, more processing overhead, neglected traffic congestion, overhearing nature, reduced communication effectiveness etc. To overcome certain short comings, we are here designing a novel approach based on network conditions to detect malicious nodes in the wireless sensor network.

3. PROBLEM STATEMENT

In most of the current WSN routing protocols, authors have applied node parameters to make routing decisions, such as residual energy, packet drop per node, connection consistency, congestion probability, etc. Interestingly, the authors have used the single parameter of the network state to make routing decisions; On the other hand, even an interrupting node may also affect overall network output (say, malicious node or outlier node). Malicious nodes may have adequate (resembling) node parameters that resemble real nodes whose inclusion in the forwarding path can lead to a drop in the packet, energy exhaustion, delay, data loss, etc. Therefore, to ensure QoS provision in WSN, in addition to the network condition aware routing decision, malicious node detection, and avoidance must be ensured. To achieve the principle of network mining, exploring various nodes as well as network parameters over the operating period can help detect malicious nodes to prevent them and make optimal decisions about adaptive routing.

This paper develops a highly robust node profiling and malicious node identification model based on network awareness that ultimately allows secure, QoS-centered, and energy-efficient routing in

WSNs. The proposed model includes a distributed time division-based node and allied connection monitoring strategy as an optimal solution that mines over the node as well as network statistics to detect malicious nodes and make optimal decisions on routing. It is possible to define the overall proposed model as a technique where Network Condition-based Node Profiling and Malicious Node Identification is carried out to identify malicious nodes. In this using the Bayesian model initially deploying nodes around the network, microlevel network evaluation was conducted where dynamic node statistics were mined and learned to identify malicious nodes. Noticeably, the proposed method hypothesis in this approach that a malicious node may either wish to drop packets, refuse services, or predict false information to cause loss of packets or degradation of efficiency.

4. PROPOSED SYSTEM

Here we are basically discussing the overall proposed method and its simulated implementation. As we stated before, our research work basically ensures to enhance the efficiency of the optimal network condition awareness with a mobile node or network mining for malicious node identification. Network Condition Based Malicious node basically aims to identify the malicious node by mining the node or network parameter. since our proposed method designs dynamic routing decisions by applying many network conditions/parameters. In the meanwhile, understanding the importance of identifying the malicious node is a vital factor in enhancing the network performance because malicious node resulting packet loss and often drop the data packets, it causes retransmission of the same packets results in more energy consumption. With this motivation, we are identifying the malicious nodes and avoiding them from routing to reduce the energy exhaustion due to malicious nodes. The detailed discussion of initial network design and deployment is given below.

4.1. Probabilistic WSN Deployment

As stated, to deploy the overall WSN network considering the probabilistic nature of the node behavior we have applied the Bayesian concept in which we construct a direct acyclic graph. In this paradigm, each connected node in the acyclic graph states a random variable, where the direct links are chosen in such a way that the combined probability distribution of the connected nodes could be obtained as the product of the conditional probability of each node in the (acyclic) graph. With such conditional deployment, a network can be stated to be a Bayesian Network.

The deployed WSN network can be stated to be a hierarchical network with multiple layers containing sensor nodes, links, branches, paths, and connectivity. Noticeably, in the deployed network, the term called “Node and/or allied Link” signifies that the variable pertaining to a node can be 1 only when it is available or able to communicate. In case of a node is not available to make communication, in the Bayesian network model it is labeled as “0”. “Branch” states that a node in Bayesian network deployment can be “1” only when the connected nodes and allied links are available, else it is labeled as “0”. Similarly, “Path” signifies that each connected sensor node is liable to provide a reliable path connecting source to the best forwarding paths generated. The other layer of the Bayesian network (Figure 1) “Connectivity” states the connectivity between the selected nodes to constitute the best forwarding path. In such network deployment, one assumption always prevails that the availability of a sensor node is always independent of the other. Similarly, the availability of a link is always independent of others.

In our proposed model, the likelihood of the first layer is characterized in terms of the availability of each node or link. On contrary, the 2nd and 3rd layers hypothesize a deterministic model signifying any link or path can work only when its connected sensor nodes function. In other words, a path can work only when its conditional probability is 1. In this manner, our proposed routing model obtains the path variables. The 4th layer of the Bayesian model variable signifies the service state of node signifying 1 when the node is connected to the forwarding path or not (i.e., 0). Thus, with respective conditional probability values, we obtained the node connectivity and availability information.

4.1.1. Asymmetric IEEE 802.15.4 MAC Information

The source node can experience dynamism with respect to traffic congestion, link failure, node failure/dead node causes packet drop at its IEEE 802.15.4 MAC layer. Generally, the major causes for packet drop are traffic congestion and out of communication range at IEEE 802.15.4 MAC layer. Such data packet drops happen due to the unavailability of information at the source node; hence this information availability plays a major role in QoS-centric routing decisions. Malicious nodes may deliver ambiguous or wrong MAC information the leads to drop packets/packet loss, and by identifying such node performing false MAC information exchange and data packet loss can be detected as a malignant node or intrusion node.

In the basic WSN protocol stack, at IEEE 802.15.4 MAC layer a source node will transmit the data and receives an acknowledgment from the identified receiver. In the meanwhile, sink node will receive the data and transmits an acknowledgment to the targeted source node. Link quality information is also a major key network characteristic ensure QoS centric routing decision, so getting link information by forwarding the probe message is important. In this mechanism each node should transmit probe message to get the link information, it is an extra energy utilization process. In our proposed model we highlight on leveraging the beacon message to avoid energy and resource utilization.

In the proposed method, every node transceiver its node characteristics to its adjacent node at each interval of 10 seconds. To allow dynamic routing, in our proposed routing protocol, every involving node exchanges its link information with one hop distant adjacent node. It can be done by using a predefined number of beacon messages. In our proposed protocol, each sensor node continues the transmission of beacon messages from one hop adjacent node. By receiving an expected number of beacon signals from the adjacent node calculate the link quality for forwarding routing decision. On the other hand, the node which transmits a number of irregular acknowledgments to its adjacent node and drops data packets will be identified as a malicious node.

Sensor node which does not receive the expected number of any signals(beacon/acknowledgment) will be identified as the intruder node or malignant node or misbehaving node. In this sense, an involving sensor node A can evaluate the likelihood of node efficiency and successful delivery probability to targeted destination Z. By applying the calculated link quality information between the nodes will be used in the forwarding routing decisions. In our proposed model, the probability of successful delivery by the node at IEEE 802.15.4 MAC layer will be calculated using (1).

$$PSD_M = \frac{\xi_{Rec(t_{i-1},t_i)}}{\xi_{pre(t_{i-1},t_i)}} \tag{1}$$

In (1), ξ_{Rec} represents the overall number of beacon signals received, and ξ_{pre} represents the overall predicted beacons during $\left(t_{i-1}, t_i\right)$ time interval.

4.1.2. Queuing Overflow

Congestion in a WSN occurs due to exceeding the buffer capacity of a traffic load of a node or link. Congestion may take place due to several reasons like unfair utilization of network resources, abrupt payload increase, topological variations, etc. If the traffic capacity increases greater than the predefined threshold, it results in the dropping of packets and retransmission makes energy exhaustion and violation of QoS.

A participating node in the communication exposing queuing delay and traffic congestion data will be identified as a malevolent node, which is not allowed to participate in the route formation. In our proposed model, we are identifying Malevolent node by examining the traffic intensity of each participating node. In our proposed model, the forwarding node gathers and monitors the traffic

statistics of each connected adjacent node. Here to gather the load traffic information of each node and congestion of each connected node, we calculate the length of the queue at the MAC layer and broadcasts this data as ack to all adjacent nodes. Let, p be the one-hop distant sensor node, while l_q be the q^{th} model cost indicating the length of the queue at a certain time interval. Here, with QL represents the total queue length samples with a certain simulation period. we calculate the average traffic load at each node using (2).

$$TL_{load\_p} = \frac{1}{QL}\sum_{q=1}^{N} l_q \tag{2}$$

Here, l_{hig} represents the highest queue length of each node at MAC layer and the total traffic density at a node is obtained using (3).

$$TL_{loadDens\_p} = \frac{TL_{load\_p}}{l_{hig}} \tag{3}$$

In our proposed protocol, the vibrant value of $T_{loadDens\_p}$ have been calculated or feed to get probability of successful transmission by a node, P_{Suc_p}, as given in (4).

$$P_{Suc\_p} = \left[1 - TL_{loadDens\_p}\right] \tag{4}$$

In our proposed routing protocol, a small Total Load Density (TLD) will be considering and for the forward routing selection, a node with a small TLD will be selected. We are obtaining the MAC Information, its regularity information at the IEEE 802.15.4 MAC layer and Successful packet delivery probability. In addition to this our model also calculate some other network constraints which will be changing with dynamic topology conditions

4.1.3. Dynamic Topology

In trust-based WSN transmission, a sensor node transmits or routes to the immediate next node only by assuring that it does not force any overhearing to the adjacent nodes. In case, if the node is capable of overhearing to the adjacent node, it is classified as a fair or normal node; else it is named as a malevolent node. Network condition in which a sensor node cannot catch the retransmission of its packet or the destination node is inaccessible because of stale or repeated forwarding data, this forwarding node is identified as malevolent or intruder node.

Here we calculate the dependability of each interested or associated node in WSN by utilizing the parameters called the Link Index Change Rate (LICR). For an associated node p, we calculate the LICR using (5).

$$\eta_p = \gamma_p + \delta_p \tag{5}$$

In equation (5), $^{3}_{p}$ represents the Rate of Link Arrival (RLA), δ_p represents the Rate of Link Outage (RLO) by p th node (). Considering the most possible RLA $^{3}_{p\_Max}$ can be equivalent to the

RLO, we acquired the maximum (δ_{p_Max}) as $^{3}{}_{p\_Max} + \delta_{p\_Max} = 2.\tilde{A}_{p}$. Like this, we calculated LICR as (6).

$$\eta = \frac{\gamma_p + \delta_p}{2.\sigma_p} \tag{6}$$

By calculating above said parameters NCAMND methodology gets the probability of effective packet transmission by a sending node by using the below formula (7).

$$PT_{\eta} = 1 - \eta \tag{7}$$

Above formula (7) uncovers the maximum LICR exhibits more dynamic adjacent network condition and subsequently, a contributing node can be identified as a malevolent node. In this way, getting the above expressed node/network parameters our designed model recognizes the malevolent node/ intruder node in an effective manner.

5. RESULTS AND DISCUSSION

Our research mainly concentrates on enhancing the Quality-of-Service provisioning in WSN. To accomplish this, we designed a solution by taking key parameters as discussed here. Malicious nodes or Outliers are dangerous in WSN, so these nodes are identified by using dynamic node or network parameters. It will help to avoid packet loss likelihood and retransmission which intern reduces energy exhaustion.

To examine the efficiency, we have compared the performance of the proposed with a recently proposed evolutionary computing named Cuckoo Search and Harmony Search (HS) based routing protocol for WSN (Swarna Priya et al., 2020). Noticeably, unlike our proposed routing where both malicious neutralizations, as well as optimal routing decision, is considered as an eventual goal, Improved Cuckoo Search and Harmony Search (iCSHS) based meta-heuristic Algorithm (Swarna Priya et al., 2020) primarily focus on achieving energy-efficiency by identifying optimal forwarding node and path in multi-hop transmission scenario. This approach considered four network parameters residual node energy, degree of a node, intra-cluster distance, and coverage ratio to perform routing. However, the initial parameters such as degree of a node, inter-node distance and coverage are used for clustering while residual energy is used for path planning for inter-cluster communication. In this approach, Cuckoo search was applied mainly to perform CH estimation, while Harmony Search (HS) performed inter-cluster routing decision by applying above stated key network parameters (residual node energy, degree of a node, intra-cluster distance, and coverage ratio). Like our proposed routing protocol, HS based routing approach at first estimates its hop-count from the destination node, which is followed by the estimation of probability factors $P_{(i,j)}$, which signifies whether a neighboring node or next-hop node j should be considered for path planning or not. Mathematically, the source node i estimates $P_{(i,j)}$ using (8).

$$\mathrm{P}\left(\mathrm{i},\mathrm{j}\right) = \begin{cases} \dfrac{\mathrm{h_i}}{\sum_{\mathrm{k}\in \mathrm{N_i}} \mathrm{h_k}} \times \dfrac{\mathrm{E_i}}{\sum_{\mathrm{k}\in \mathrm{N_i}} \mathrm{E_k}} & \text{if } \mathrm{j} \in \mathrm{K} \\ 0 & \text{else} \end{cases} \tag{8}$$

In (8), the parameter where N_i states the set of neighboring nodes, while h_i and h_k presents the number of hop-counts from the source node (i) and neighboring node or adjacent node j, respectively. Thus, obtaining the hop counts and eventual. Initializing the HM heuristic model, the energy consumption of energy path (9) is obtained and a path with the highest consumption is labeled as P_{worst}. In computational evolution a new path X^1 is created based on a certain Harmony memory consideration rates (HMCR) (here, HMCR=0.7). For the first node in the path X as the source node, to select the next-hop node or neighboring node HS generates an arbitrary number between 0 and 1. In case the value of X^1 is less than HMCR (0.7) then the next-hop node is selected from another column. Otherwise, that node is considered as the next-hop node to constitute a forwarding path.

$$HM = \begin{Bmatrix} X_1 \\ X_2 \\ . \\ . \\ . \\ X_i \\ . \\ . \\ X_{HMS} \end{Bmatrix} = \begin{Bmatrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{Bmatrix} \begin{matrix} \left(s, x_{1,2,}, \ldots, \ d\right) \\ \left(s, x_{2,2,}, \ldots, \ d\right) \\ . \\ . \\ . \\ \left(s, x_{i,2,}, \ldots, \ d\right) \\ . \\ . \\ \left(s, x_{HMS,2,}, \ldots, \ d\right) \end{matrix} \tag{9}$$

This process is continued till a complete path between source and destination is not formed. Additionally, iCSHS uses an additional attribute called Pitch Adjustment Rate (PAR=0.8), where to enhance path reliability each path is compared with PAR and if it falls below PAR, a random node from the path is substituted by the neighbor node and this process continues till an optimal path is obtained. A detailed discussion of the results obtained is given as follows. Noticeably, to enable the better presentation of the results the NS2 based simulated outputs have been converted into MATLAB, which are depicted in Figure 1, Figure 2, and Figure 3.

In this paper, we are designing an efficient approach by the name Network Parameter based Malicious Node Detection to yield Quality of Service centric routing. It uses various dynamic node and/or network parameters such as successful data delivery ratio, irregular MAC information, and data overflowing to perform malevolent node detection. So, this robust implementation of the proposed method will enable reliable and QoS centric data communication in WSNs. The proposed model is implemented using the network simulator NS2 development platform. The simulation variables and underlying experimental setup values taken in this work are as follows. Considering 49 nodes deployed over the WSN dimension of 100X100 for the network design and simulation. IEEE 802.15.4 Mac protocol is used between the network and physical layer, IEEE 802.15.4 PHY protocol is used at the physical layer. A radio signal of 200 meters is considered with a transmission rate of 10-512 packets per second. We used career frequency of 2.5GHz, the antenna used here for transceiver function is an omnidirectional antenna. It uses the efficiency of RF power amplifier value of 0.47, transmission

channel factor of 30dB, the power density of radio channel is -130 dBm/Hz. At the receiver side noise factor taken is 10dB and the bit error rate is 10^{-3}dB. The transmitter circuit consumes 98.2 mW power, a packet size of 512 Kbytes, and an antenna gain of 5dB.

Figure 1 exhibits the delay incurred in both approaches. As already indicated, the iCSHS model at first applies Cuckoo search to perform clustering optimization, which is then followed by HS based routing decision where it performs two-stage iterative node and path verification. This overall process increases latency. On contrary, our proposed routing protocol obtains network parameters dynamically and updates the same in a proactive manner, which helps the proposed model to perform the respective tasks efficiently. It makes our proposed routing protocol time-efficient, which is vital for any contemporary WSN based communication systems.

Observation of the overall system performance inferred that the proposed method achieves better reliability, a higher success rate of transmission, low energy consumption, and end-to-end delay. It makes our proposed system suitable for real-time WSN routing purposes. The overall research inference is given in the subsequent section. As stated, iCSHS model is the computationally exhaustive approach and hence is supposed to incur high energy consumption during clustering optimization and subsequent path planning. It makes iCSHS undergo high energy consumption. On contrary, our proposed model preserves energy contributed due to low or reduced computational complexity and retransmission probability (Figure 2).

As stated, iCSHS model is the computationally exhaustive approach and hence is supposed to incur high energy consumption during clustering optimization and subsequent path planning. It makes iCSHS undergo high energy consumption. On contrary, our proposed model preserves energy contributed due to low or reduced computational complexity and retransmission probability. Our proposed model reduces energy consumption by reducing the queuing delay which is common in a busy network. Retransmission will consume more energy in the network, it can be done by the result of having outlier nodes in the network.

Figure 1. End-to-End delay Vs node density

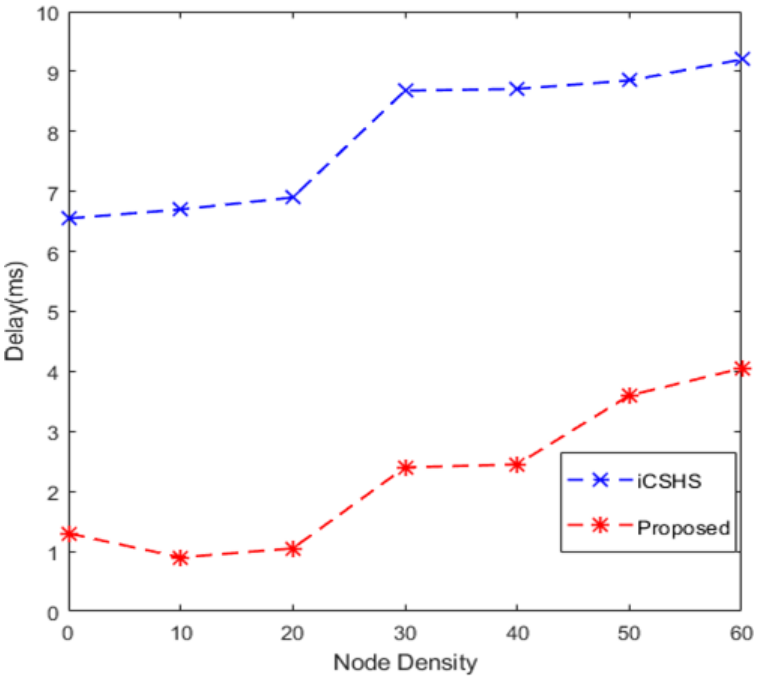
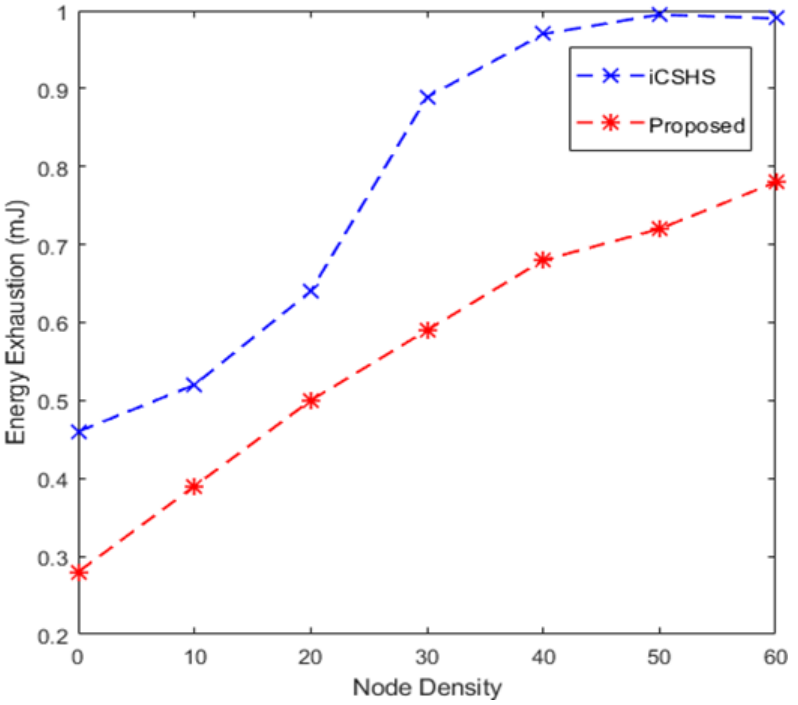


Figure 2. Energy exhaustion or consumption Vs node density



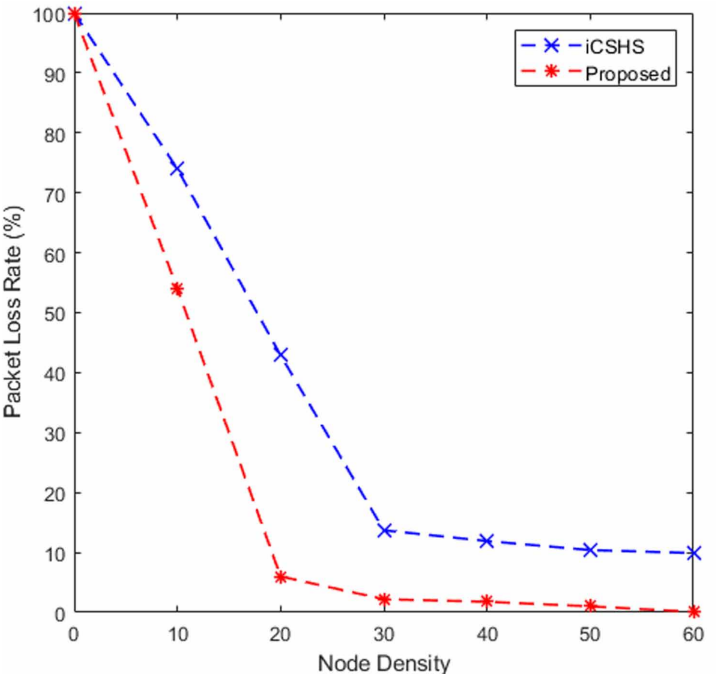
So, in our proposed model we are identifying then outlier nodes based on three network conditions like Asymmetric IEEE 802.15.4 MAC information Exchange, Queuing Overflow, and Dynamic Topology. So, the retransmission possibility is less because of these features. In this conjunction, considering packet loss performance we find that the proposed routing model exhibits low loss as compared to iCSHS protocol. The influence of such robustness can be easily envisaged in Figure 3, where NCBOD has shown lower Packet loss due to packet drop as compared to iCSHS protocol.

Thus, by observing the overall performance of our proposed system, it can be inferred that the proposed method achieves better reliability, a higher success rate of transmission, low energy consumption, and minimum end-to-end delay. It makes our proposed system suitable for real-time WSN routing purposes.

6. CONCLUSION

The current era of the smart world having a huge demand for IoT devices and utilization of these devices in an energy-efficient and reliable manner. The quality of service is an important security goal of data communication, it should be achieved in the machine-to-machine and smart IoT communication. In this paper, we are considering the dynamic nature of the wireless sensor network to collect various dynamic parameters to accomplish QoS. Here we are presenting an optimal routing protocol based on the network conditions i.e. Network Condition Based Malicious node detection protocol. This exploits various network conditions such as dynamic or irregular MAC information exchange, queuing overflow probability of True positive data delivery to detect the malevolent node. This approach yields reliable data transmission, avoids delay in transmission, reduces packet loss, retransmission probability will be reduced, and hence achieved with energy efficacy. It also reduces the computational cost by ensuring high reliability and Quality of Service provision. The implementation of our proposed protocol is tested in network simulator NS2. It shows the reduction in packet loss due

Figure 3. Packet Drop (%) Vs node density



to malicious node detection with the IEEE 802.15.4 protocol standard. It also shows the proposed method is suitable for real-time applications. In the future enhancement, the link connectivity and availability of a node can be considered to design an effective optimal routing using any machine learning algorithm. The malevolent patterns can be converted as the knowledge to train the network, it enables time-efficient routing decision in future steps by not repeating the same detection process.

REFERENCES

Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A., & Awajan, A. (2020). Intelligent mobile malware detection using permission requests and API calls. *Future Generation Computer Systems, 107*, 509-521. 10.1016/j.future.2020.02.002

Azlan & Al-Anbuky. (2015). Modelling the Integrated QoS for Wireless Sensor Networks with Heterogeneous Data Traffic. *Open Journal of Internet of Things, 1*(1).

De Paola, S. (2015, May). Adaptive Distributed Malevolent Detection for WSNs. *IEEE Transactions on Cybernetics*, *45*(5), 902–913. doi:10.1109/TCYB.2014.2338611 PMID:25073183

Ehsan, S., & Hamdaoui, B. (2012). A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks. IEEE Communications Surveys & Tutorials, 14(2), 265-278. doi:10.1109/SURV.2011.020211.00058

Feng, Liang, & Lei. (2017). Distributed Malevolent detection algorithm based on credibility feedback in wireless sensor networks. *IET Communications, 11*(8), 1291-1296.

Gupta & Jha. (2018). *Integrated clustering and routing protocol for wireless sensor networks using Cuckoo and Harmony Search based metaheuristic techniques*. DOI:10.1016/j.engappai.2017.11.0.-2018

Hang, , Chao, , Chen, , Shu, , Park, , & Park, . (2010, December). Malevolent detection and countermeasure for hierarchical wireless sensor networks. *IET Information Security*, *4*(4), 361–373. doi:10.1049/iet-ifs.2009.0192

Kachouri & Mahfoudhi. (2016). Anomaly detection through Malevolent and neighborhood data in Wireless Sensor Networks. *2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP),* 26-30.

Kachouri & Mahfoudhi. (2017). Malevolent detection for wireless sensor networks using density-based clustering approach. *IET Wireless Sensor Systems, 7*(4), 83-90.

Khan, R., Ali, I., Zakarya, M., Ahmad, M., Imran, M., & Shoaib, M. (2018). Technology-Assisted Decision Support System for Efficient Water Utilization: A Real-Time Testbed for Irrigation Using Wireless Sensor Networks. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 25686–25697. doi:10.1109/ACCESS.2018.2836185

Kumar Dwivedi, R., Pandey, S., & Kumar, R. (2018). A Study on Machine Learning Approaches for Malevolent Detection in Wireless Sensor Network. *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence),* 189-192.

Li, W., Bassi, F., Dardari, D., Kieffer, M., & Pasolini, G. (2016, March). Defective Sensor Identification for WSNs Involving Generic Local Malevolent Detection Tests. *IEEE Transactions on Signal and Information Processing Over Networks*, *2*(1), 29–48. doi:10.1109/TSIPN.2016.2516821

Liu, H., He, J., Rajan, D., & Camp, J. (2013). Malevolent detection for training-based adaptive protocols. *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, 333-338. doi:10.1109/WCNC.2013.6554586

Martins, H., Januário, F., Palma, L., Cardoso, A., & Gil, P. (2015). A machine learning technique in a multi-agent framework for online Malevolents detection in Wireless Sensor Networks. *41st Annual Conf. of the IEEE Indus. Elect Soc*., 688-693.

Medeiros de Ara'ujo, G., & Becker, L. B. (2011). A Network Conditions Aware Geographical Forwarding Protocol for Real-Time Applications in Mobile Wireless Sensor Networks. *2011 IEEE International Conference on Advanced Information Networking and Applications*, 38-45.

Numan, M., Subhan, F., Khan, W. Z., Hakak, S., Haider, S., Reddy, G. T., Jolfaei, A., & Alazab, M. (2020). A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 65450–65461. doi:10.1109/ACCESS.2020.2983091

O'Reilly, C., Gluhak, A., Imran, M. A., & Rajasegarar, S. (2014). Anomaly Detection in Wireless Sensor Networks in a Non-Stationary Environment. IEEE Communications Surveys & Tutorials, 16(3), 1413-1432. doi:10.1109/SURV.2013.112813.00168

Rajasegarar, S., Leckie, C., Bezdek, J. C., & Palaniswami, M. (2010, September). Centered Hyperspherical and Hyperellipsoidal One-Class Support Vector Machines for Anomaly Detection in Sensor Networks. *IEEE Transactions on Information Forensics and Security*, *5*(3), 518–553. doi:10.1109/TIFS.2010.2051543

Sen, J., & Ukil, A. (2009). An adaptable and QoS-aware routing protocol for Wireless Sensor Networks. *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 1st International Conference*, 767-771. doi:10.1109/WIRELESSVITAE.2009.5172546

Spachos, P., Toumpakaris, D., & Hatzinakos, D. (2015). QoS and energy-aware dynamic routing in Wireless Multimedia Sensor Networks. *Comm., 2015 IEEE International Conference*, 6935-6940. doi:10.1109/ICC.2015.7249431

Sutaone, M., Mukherj, P., & Paranjape, S. (2016). Trust-based Cluster head validation and Malevolent detection technique for Mobile Wireless Sensor Networks. *2016 International Conference on Wireless Communications, Signal Processing and Networking Chennai*, 2066-2070.

Swarna Priya, Maddikunta, Parimala, Koppu, Gadekallu, Chowdhary, & Alazab. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications, 160*, 139-149. 10.1016/j.comcom.2020.05.048

Wang, Z., Song, G., & Gao, C. (2019). An Isolation-Based Distributed Malevolent Detection Framework Using Nearest Neighbor Ensembles for Wireless Sensor Networks. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 96319–96333. doi:10.1109/ACCESS.2019.2929581

Xu, S., Hu, C., Wang, L., & Zhang, G. (2012). Support Vector Machines Based on K Nearest Neighbor Algorithm for Malevolent Detection in WSNs. *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing,* 1-4.

Yessembayev, D. (2018, September). Detection of Good and Bad Sensor Nodes in the Presence of Malicious Attacks and Its Application to Data Aggregation. *IEEE Trans. on Signal and Information Processing over Networks*, *4*(3), 549–563.

Yu, T., Wang, X., & Shami, A. (2017, December). Recursive Principal Component Analysis- Based Data Malevolent Detection and Sensor Data Aggregation in IoT Systems. *IEEE Internet of Things Journal*, *4*(6), 2207–2216. doi:10.1109/JIOT.2017.2756025

Zhang, H., & Li, Z. (2019). Anomaly Detection Approach for Urban Sensing Based on Credibility and Time-Series Analysis Optimization Model. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 49102–49110. doi:10.1109/ACCESS.2019.2909967

Zhang, Y. (2010, December). Malevolent detection and countermeasure for hierarchical wireless sensor networks. *IET Information Security*, *4*(4), 361–373. doi:10.1049/iet-ifs.2009.0192

Sunitha R. is currently working as an Assistant Professor in the Department of Computer Science & Engineering, PES University, Ring Road Campus, Bangalore, Karnataka, India May 30, 2019 - Till date Worked as an Assistant Professor in the Department of Computer Science & Engineering, Malnad College of Engineering, Hassan, Karnataka, India April 02, 2014 – May 29, 2019 Member of Center for Information Security, Forensics and Cyber Resilience (ISFCR) and Center for Internet of Things. Pursuing Ph.D. in Computer Science & Engineering, Malnad College of Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India admitted in 2016.

Chandrika J. (PhD) is a professor for the Department of CSE at Malnad College of Engineering, Salagame Road, Hassan. Teaching experience is about 30 Years Research experience is about 9 years Broad Area of Research work: Data Mining and Analytics- Applied data mining techniques for handling ubiquitous stream data. This has a very broad range of applications like handling medical data, sensor data, satellite data, etc. The research conducted has proposed a novel framework and applied this framework for frequent itemset mining and clustering techniques. The outcome published in many refereed journals and conferences. Around 40 research papers published in various reputed journals and conferences. One Ph.D. scholar awarded and is presently guiding 4 scholars.