I J C T A, 9(34) 2016, pp. 817-832

Efficient Path Reassessment Based on Node Probability in Wireless Sensor Network

[1]C. R. Rathish and [2]A. Rajaram

ABSTRACT

A wireless sensor network is a group of distributed autonomous devices using sensors with a communications infrastructure for observing and capturing conditions at various sites. Use of wireless sensor networks and interaction nature of the network protocols make such network unprotected to various forms of attacks, where malicious nodes are deployed into the network and cause many attacks. These nodes are considered as compromised nodes and it brings the bad mouthing attack and it makes the network performance progressively worse. This system works based on the study of picking the best path selection based on the probability of nodes. An Efficient Enhanced Route Reassessment Algorithm (EERRA) is proposed for route selection, this identifies the high priority and low priority nodes in the network. High priority nodes has high packet delivery ratio and low priority nodes are avoided as it combines with bad-mouthing attack. In case of any low priority nodes are identified during path selection, the algorithm reassesses the path of network. The proposed work constitutes three phases. In first phase, we monitor for the bad mouthing attack that interfere in the network. In second phase, the algorithm removes the low priority nodes that acts as malicious and cause congestion in the network. In third phase, efficient enhanced route reassessment algorithm picks the suitable path by considering the probability of sending and receiving the packets in the network and enables the route selection is conducted flexibly and adjusted according to the requirements. This greatly reduces the congestion and improves the path stability in the network. The simulation result shows the reduced rate of communication overhead and reduces the energy consumption. The performance analysis of proposed EERRA improves the connectivity, network lifetime, packet delivery ratio.

Keywords: Path Reassessment, Bad-mouthing attack, Node Probability, Congestion, Efficient Enhanced Route Reassessment Algorithm.

I. INTRODUCTION

Mostly many wireless sensor networks (WSNs) are located in unguarded surroundings in which restoring energy is tough if not impossible. Owing to limited resources in wireless sensor network, the energy consumption must be reduces to improve the network life time and stable path. Network congestion reduces the quality of service when the nodes carry more data than it can handle. Congestion control plays an important role that helps in preventing loss of packets in network traffic. Various types of data are produced by the nodes have different priorities. It is necessary to know the sufficient transmission rate for each node in the network. That is every node knows the probability of sending and receiving the packets in the network. And also the nodes should not malicious for effective transmission of data. Hence monitoring the malicious nodes helps in eliminating the compromised nodes in the link. Removing low priority nodes and compromised nodes are the two major factors for the successful route selection.

In wireless sensor network, several factors are involved in the congestion includes buffer over flow, packet loss, reducing network throughput and wastage of energy. To address these issues in wireless sensor

[1] Research Scholar, St. peter's University, Chennai, India

[2] Professor, Department of Electronics and Communication Engineering, EGS Pillay Engineering College, Nagapattinam, India

E-mail: [1]r.rathish87@gmail.com, [2]gct143@gmail.com

network, a distributed algorithm is introduced [1] that relieve congestion and assign proper source rate to a sink node. It provides the ideas hop-by-hop congestion control and end-to-end congestion control for how to control and manage the traffic occurs in the network. Hop-by-hop method has faster response and difficult to adjust the intermediate node transmission rate. End-to-end method has slower response and force the transmission rate at every source node and it simplifies the design at each intermediate nodes.

A probability model [2] is provided for network lifetime, it assumes Poisson distribution is used for packet generation, and all the nodes have similar packet generation model, initial energy and random deployment, and complementary cumulative density function is obtained for both single-hop and multi-hop wireless sensor networks that finds the accurate probability of network achieves given lifetime. It analyzes the lifetime at sensor level instead of assuming it, so it can be used to design both network and node parameters related to desired lifetime. Due to fault nodes, the data collected by sensor might be wrong. It is important to find events in the existence of wrong sensor readings and incorrect reports. A neighbor-based malicious node detection scheme [3] is introduced to detect the faulty nodes. Every sensor nodes make a decision on fault status of itself and neighbor nodes depend on the sensor readings. Most of erroneous results because of transient faults are rectified by filtering and permanent fault nodes are eliminated using confidence-level evaluation, to enhance malicious node detection rate accuracy. High event detection accuracy is preserved by keeping track of past events reporting records.

In order to avoid all these issues, proposed system introduces the Efficient Enhanced Route Reassessment Algorithm in this work. This work comprises of three phases. In first phase, it monitors for bad mouthing attack that reduce the performance of the network. To identify the malicious nodes, the trust value of every suspicious pair is compared with the network pre-defined threshold value. In second phase, the algorithm identifies the low priority nodes by keep track on the probability of nodes and eliminates the low priority nodes from the link. In third phase, algorithm picks the optimal path by considering the probability of sending and receiving the packets in the network and enables the route selection is conducted flexibly and it reduces the congestion to a greater extent and improves the path stability in the network.

The organization of this presented work is as follows. In Section II related work on congestion control and malicious node detection are analyzed. The details of proposed Efficient Enhanced Route Reassessment Algorithm (EERRA) explained in section III. The simulation results of proposed work are shown in section IV. The paper is concluded in section V.

II. RELATED WORK

In this section, survey about congestion control, probability of network for efficient data transmission and how to monitor the malicious or compromised nodes are analyzed. Shintaro Mori [4] presented an efficient cooperative sensing data collecting using unmanned aircraft vehicle in wireless sensor network. The architecture is proposed with MAC protocol that explains how to choose the target cooperative sensor node and which data to be retransmitted using the decided cooperative sensor node. By using the exhaustive monte carlo computer simulations, the sensing data are collected accurately with the improved probability. The results shows that the scheme works effectively if the number of sensor nodes is satisfied with $1{,}000 \leq N \leq 5{,}000$ regions and the proposed work is improved by 16.3%, 46.8%, 49.8%, 74.2% and 92.6% if N=1000, 2000, 3000 and like on.

Ying Tian [5] analyzed that coverage is one of the significant issue in wireless sensor network that measures the quality of services from sensors deployed in the sensing region. The proposed work presented a node schedule method for multi coverage probability based on the probabilistic coverage in wireless sensor network is more realistic comparing with the other traditional detection model. In the proposed work, the coverage problems are investigated based on multi-coverage requirement. By setting the backoff

time the sleeping sensors in the hot areas are become active. The simulation results of this study shows that nodes are work effectively comparing with the existing protocols.

Adwan Alanazi [6] studied the various quality of service routing methods focus on improving throughput and transmission delay in wireless sensor networks. Data traffic can be composed into reliability demanding and time sensitive packets of data in wireless multimedia sensor networks. In that situation, load balancing and optimization of node improve the quality of service provisioning. Hence the optimized node selection process is introduces in the proposed work which helps in flexible route discovery using residual energy and received signal strength indicator for improving quality of service. The proposed approach increases the lifetime of network, throughput, end-to-end delay, and avoid bottlenecks.

Alberto Gallegos [7] analyzed the unbalanced energy consumption among the sensors in wireless sensor networks. The proposed work presents the simulation study of maximum amount shortest path routings using Ns-3 in wireless sensor networks. Maximum Amount Shortest Path routing protocol using sink mobility with constrained paths and reducing the message flood by limiting the flood area improves the energy efficiency in wireless sensor networks. This protocol is table-driven in nature and collect large amount of data in least energy. It uses constrained paths and divides the deployed sensor nodes into independent zones in order to construct the routing tables. The performance evaluation of Ns-3 provides better performance.

Zhenjing Zhang [8] studied an issue in the delay tolerant network that selfish nodes are not willing to transmit the message from strangers and the malicious nodes that reduce the performance of network. The proposed work that introduces a trust based efficient routing to address these security issues in the social delay tolerant network. This introduced a dynamic trust model that prevents bad-mouthing attack and ballot stuffing attacks. In order to avoid blackhole and greyhole attacks, Shannon entropy function is introduced which improves the performance of network.

Antesar M. Shabut [9] deals with building a trust model that adopts recommendations by other nodes in the network is a challenging issue because of the risk of untrust recommendations like bad-mouthing, ballot-stuffing, and collusion. The important issue in the mobile ad hoc network is the reliability of receiving packets in multi-hop intermediate nodes, may include malicious and misbehaving nodes. Hence a recommendation based trust model is introduced to filter out the compromised nodes in the period of searching for a packet delivery route that employs clustering technique to dynamically filter out attacks associated with dishonest recommendations between certain time depends on number of interactions, similarity of information and closeness between the nodes. The model is really examined under many mobile and disconnected topologies in which nodes practices changes in their neighbour leading to repeated route changes. This indicates strength and perfection of the trust model in a dynamic mobile adhoc network environment.

Jiajing Wu [10] introduces the node usage probability from compound networks by studying the traffic performance in communication networks from the complex networks. These characteristics the traffic load distribution and investigates how repeatedly a node is selected to relay packets in the network. By using this probability, an efficient network design procedures, routing algorithms, resource allocation schemes are developed to improve the traffic performance. The proposed work compares the performance of proposed routing with other routing algorithms like shortest path, minimal degree routing, and effectively balance the load based on the node usage probability and achieves the optimal network performance.

Gulnaz Ahmed [11] surveyed about the algorithms in wireless body area sensor networks. The survey explains how the algorithms utilize various techniques in order to reduce energy consumption, transmission delay, and cost of path selection. The performance of MATLAB simulations analyze the path loss and consumption of energy in disconnected nodes. The connectivity between employ nodes and out body server on LOS and NLOS is also check due to frequent human body movements. The connections may also break

because of absorption of cloths and human body, and it leads to delay and more energy consumption and takes time to setup a connection. From this survey it is found that the algorithms are planned to address the problem of emergency should be priority base and can be maintain its energy range easily for sending data when partitioning cause disconnection to occurs.

Bongsue Suh [12] proposed rendezvous points and routing path selection approaches for wireless sensor networks with mobile sink to gather data from the sensor nodes. In the proposed system, the selection of RP nodes and final routing paths are depends on current information of previously selected RP nodes. The results of proposed RP node and routing path selection algorithm leads to efficient energy consumption and decreases forwarding hop counts comparing to the previous algorithms. The performance improvement of proposed approaches become more important as the number of sensor nodes improves within the sensor field.

Saima Jamil [13] studied cooperative routing is a technique that utilizes the benefits of cooperative communication at physical layer and necessary route selection in network layer, which reduces the power consumption and delay in transferring the data between two nodes. Cooperative routing decreases the effects of channel fading and improves the energy efficiency during transmission in wireless sensor networks. The proposed Cooperative power and energy efficient routing protocol is compared with the other routing protocols like LEACH and PEGASIS and found to be better results of energy efficiency, packet delivery rate and throughput and it is capable of prolonging the network lifetime.

Farah Khedim [14] surveyed in wireless sensor networks many trust and reputation models are proposed to provide effective security mechanisms. It plays an important role in protecting wireless sensor networks against insider attacks like Dos and node replication. It also faces many security issues of dishonest recommendation attacks like slandering, collusion and self-promoting. So the proposed work divides the scheme into two main categories avoiding dishonest recommendation to prevent the attacks and dealing with dishonest recommendations to detect the attacks as soon. The comparisons of this study address the drawbacks of existing protocols.

Zakirullah [15] analyzed that indirect trust is unprotected to different types of attacks from dishonest recommenders in mobile ad hoc networks. To detect the dishonest trust recommendations before utilizing it, a scheme is proposed. This scheme introduces the dissimilarity function based mechanism finds the distance of recommended trust from the mean of recommended trust which is used in smoothing function that filters outs the dishonest recommendations among the overall recommendation trust. High dissimilarity recommendations are considered as malicious. The proposed mechanism is evaluated against ballot stuffing, bad mouthing attack and random opinion attacks.

Cai Gao [16] presented a Bio-Inspired Algorithm to decide the optimal communication path in wireless sensor networks. Adaptivity is the most important feature of this algorithm. In the proposed work optimal communication path problem is constructed and transform it into shortest path tree problem and considers external base station as root node and sensors as the leaf nodes. If the edge weight changes the algorithm can reconstruct all the edges automatically. The system is high parallelism by using independent CPU of each sensor. This algorithm is proposed by the inspiration of path finding mathematical model Physarum solver and result analysis shows that it performs better than physarum solver.

Anuradha M P [17] analyzed that to monitor information in the wireless sensor network; the geographically distributed sensor nodes can cooperate with each other in order to improve the performance of data transmission. The nodes in the network can be distributed or hierarchical and it possesses same characteristics or different characteristics. A data aggregation technique is developed for all mixed conditions and presented mathematical viewpoint using probability functions and distances to restore the data. The proposed network is highly secure, inexpensive, and reliable and it carried out by only the authorized users.

Seo Hyun Oh [18] studied the limited resources in wireless sensor network leads to malicious attacks. The affected nodes or compromised nodes can send the erroneous data to base station. A malicious and malfunctioning node detection scheme is introduced to identify the faulty nodes which use dual-weighted trust evaluation in a hierarchical sensor network. Faulty nodes are identified effectively in the presence of noise and natural faults without sacrificing fault-free nodes. The simulation results of proposed scheme shows that it performs better in event detection, misdetection rate, false alarm rate and malicious detection rate than the other existing schemes.

He xin [19] presented a heider theory based reputation framework for wireless sensor network after studying that the normal mechanism related to security which is not sufficient for monitoring all types of security problems that results in malicious act. The proposed work first analyzes the problems that are caused in the unreliable wireless channel using reputation framework then it improves this framework with the heider theory which observes the mutual neighbor nodes, increases the calculation of direct reputation value when the channel is undependable and improves the accuracy of trust value. The simulation results shows that heider theory framework get exact reputation value and maintain its flexibility against bad mouthing attacks.

Zhang Mingwu [20] introduces trust metric in order to find the malicious behaviours in wireless sensor networks. To improve the transaction security in wsn, it is essential to determine the nodes trustworthiness. Compromised nodes may change their behavior to hide the malicious behavior and encouraging their status. This might modify the trust entropy in system because of their biased voting ratings. So the proposed system introduces the standard structure entropy for distributed entities which is used to identify any malicious activities that involved in the system. The simulation results explained whether the system is maliciously attacked or attacked randomly or collusively. Honest nodes are dropped by bad mouthing attack in collusive attack.

Zhibin Li [21] proposed a priority based congestion control in any multipath and multi hop wireless sensor networks. Congestion leads to packet loss and waste energy in network, and it can be avoided in weighted fairness way but it becomes more complicated due to the data flow in multiple routing paths. So joint priority based algorithm is proposed that eliminates the congestion and achieves the weighted fairness with high source priority and sends more packets in multi-path and multi hop wireless sensor networks. It defines the new variable joint priority (JP) that indicates the arithmetic mean of all source nodes that the data flows in the particular link and the rate of data flow is adjusted if there is any congestion occurs in the link. The proposed algorithm can be worked with many routing protocols.

Daniel-Ioan Curiac [22] introduced an auto regression technique in wireless sensor network to detect malicious nodes. In this technique, a strategy is provided based on past and present values of each sensor in network to identify the malicious activity. And the sensor output at every moment is compared with autoregressive predictor estimated value. The sensor node is considered as suspicious if the difference between two values is higher than chosen threshold then the decision block is activated. This technique is very easy to detect misbehaving nodes and algorithm is more suitable for large scale sensor networks.

Richa Agarwal [23] proposed a probability based energy efficient clustering protocol in heterogeneous environment of wireless sensor network. It assumes that node may vary on content of their energies, so the algorithm is effectively chooses cluster heads for formation of consecutive round clusters in the network. Nodes initial energy and left over energy are the parameters that need to consider while selecting cluster head. The probability of node to be chosen as cluster head based on these energies, as it prevents weaker nodes that is low energy nodes are die quickly or charging the single node with the responsibility of cluster head resulting in early death of that node and effectively manage the network resources.

III. OVERVIEW OF PROPOSED WORK

Security in wireless sensor networks is difficult. The proposed work mainly contributes towards monitoring the malicious nodes and selects the high priority nodes for route selection. Efficient Enhanced Route Reassessment Algorithm (EERRA) which effectively picks the routing path. This control the congestion based on the node priority in any multipath or multi-hop wireless sensor network. This section explains about three phases in the proposed work. In first phase, bad-mouthing attack is monitored in the network. In second phase, low priority nodes are removed from network and in third phase efficient path reassessment algorithm is presented.

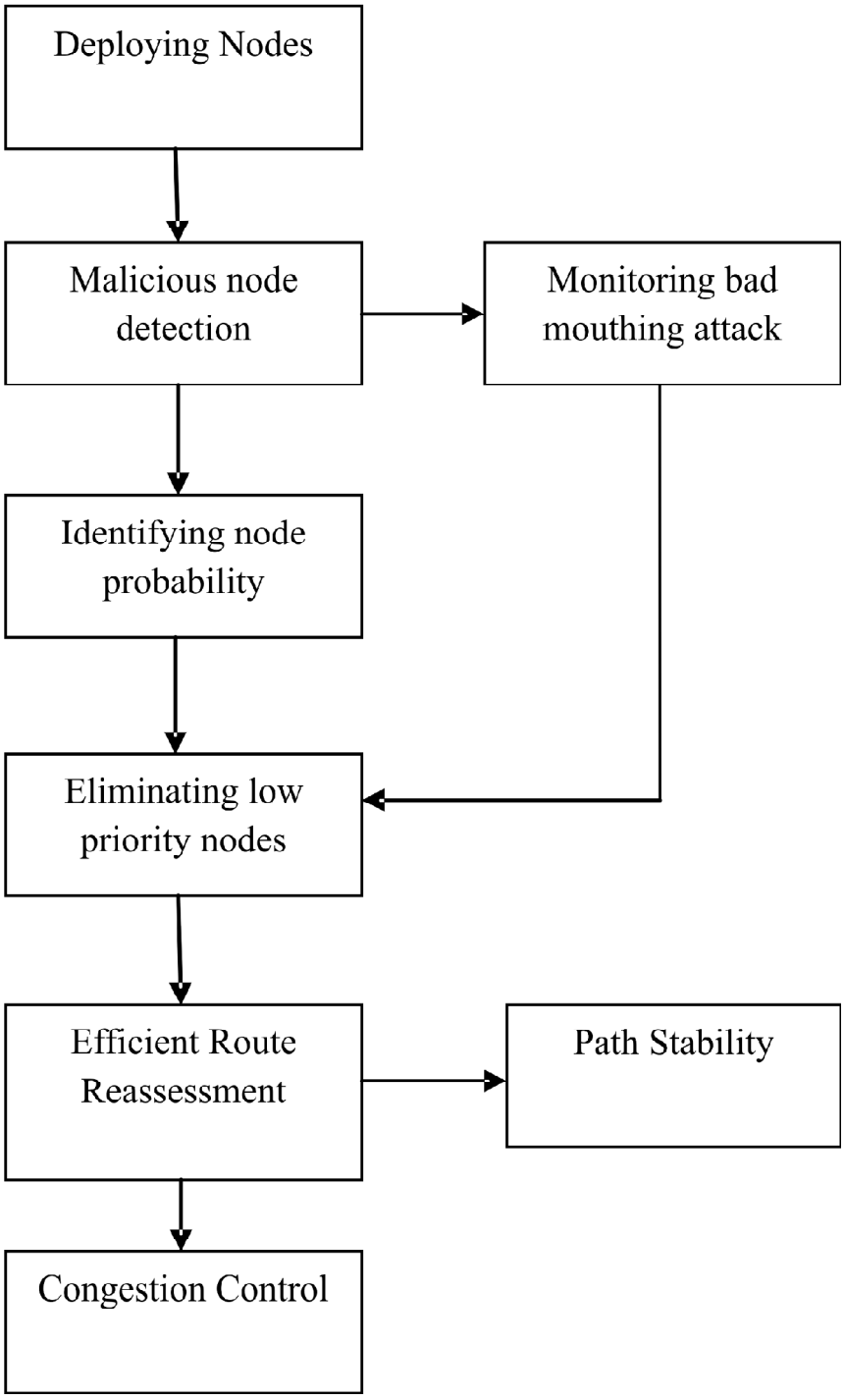

Figure 1: Block Diagram of Proposed Work

Figure 1 shows the block diagram for proposed work. Initially the network starts with nodes formation and need to monitor for any malicious nodes in the network. It is little complex to keep track of all nodes in the wireless sensor network. A sensor node may be compromised and act as malicious and provides the wrong information to other nodes and it causes the worst performance of network. Malicious nodes repeatedly send the incorrect information to their neighbor nodes. The algorithm monitors for occurrence of bad mouthing attack in the network. The malicious nodes are identified by comparing the trust value pairs with the threshold value. Then it detects the low priority nodes in the network by comparing the packet delivery ratio and removes it. The route is reassessed based on the probability of nodes selection. The effective path is picked with the shorter hops and it effectively fits for high throughput and reduces the congestion in the network.

1. Monitoring Bad-mouthing Attack

Malicious nodes interrupt the data in wireless sensor network. The main goal is to identify the nodes that act as malicious, which includes many malicious activities like modifying the packet, dropping the packet, packet misrouting, use of wrong identity and formulating other nodes to act bad in the wireless sensor networks. To pick the path without any malicious nodes, the proposed system monitors for the attack in the path.

Bad mouthing can be initiated at any moment that consists of several malicious nodes that assign false belief to nearby nodes that makes the network performance progressively worse. The protection against bad mouthing attack depends on usage of identity and trust. Trust and identity plays important role, the models is designed in a tree structure that each child node detects their parent node for forwarding the packet towards base station for successful transaction. Each child node selects own parent node based on the observation on parent node. Every child node adds its identity and trust value on parent node, and shares it with base station. Every child node transmits the packet by encrypts the bytes that added by node in packet before transmitting the packet to the parent node. Once the packet reaches the base station, and it starts decryption of the packet with pair wise keys that shared with nodes in the route. The decryption process is achieved with the shared keys from nodes in the reverse order in the forwarding path from base station to source node. Modification can be involved in two ways. The received packet is modified before adding and encrypting the marker data and also modified after adding the marker data before forwarding the packet. Base station can identify the node that acts as malicious based on the identity and trust value in the packet. Transmission of data is divided into multiple rounds of equal time duration.

If we have four nodes A, B, C and S. B is the parent node for A, C is the parent node for B. Here B receives the packet from A and forwards it to node C. Here the packet modification can takes place in any form. Either B modifies the data and sends it to node C or C modifies the data before adding the marker and transfer to S. Here S is base station which identifies the malicious node during decryption. This monitors for the malicious node continuously for the effective transmission of data.

Consider a wireless sensor network consists of N nodes. Each packet flows from source node to base station passes in the set of links. Let R = $\{r_1, r_2 \ldots r_k\}$ denote the set of transmission routes. To reach the base station, each packet pass through all nodes in the predetermined route, and some of these nodes are responsible for encoding the packets. Each child node chooses their parent node and adds its identity and trust value. Let T be the set of trust value and each child, parent pair value is given by,

$$T_{(C,P)} = (C_1, P_1), (C_2, P_2) \ldots (C_n, P_n)\} \quad (1)$$

From equation (1), $T_{(C,P)}$ denotes the trust value pair of child parent link. (C_1, P_1) be the trust value if first pair in the link, (C_2, P_2) be the next pair link and so on. Every trust value is tracked in the link and this value is compared with the network predefined threshold value in order to find the nodes that act as malicious.

2. Removing Low Priority Nodes in Network

Base station identifies the malicious nodes during decryption of packets. The low priority nodes or malicious nodes which make the performance of network poorer or the nodes that causes congestion in the network. It is important that the node should have high priority which sends more number of packets than the low priority nodes. Low priority nodes are the one which causes packet loss in the network.

The base station consists of sequence of marker information that is added by all forwarding nodes and message from the source node. The malicious node is found out with the help of trust value that is recorded for each node by child on parent node. After a single round of transmission base station contains all pairs of parent and child node and trust values. Initially, the network sets the pre-recorded threshold value and checks this value with all the suspicious pair values. The threshold value of the network is denoted by T_L. The value of $T_{(C,P)}$ is compared with the value of network threshold. The transmission route is set according to the value pair of nodes.

$$R = \begin{cases} 1, \textit{ if link exists} \\ 0, \textit{ otherwise} \end{cases} \tag{2}$$

From equation 2, it shows that the transmission route is exists based on trust value pair of child and parent node. That is transmission route is established if the trust value pair satisfies the predefined network threshold value otherwise the route is reassessed. If the trust value pair is equal to threshold value then the link is selected for packet transmission. This condition is given by,

$$T_{(C,P)} = T_L \tag{3}$$

If the value is less than pre-recorded threshold value, parent node is considered as malicious else if it is greater, child node is considered as malicious. These conditions are shown in (4) & (5). If the node is malicious, it seeks for new nodes with the shorter hops and sufficient probability of transferring packets.

$$T_{(C,P)} < T_L \tag{4}$$

Similarly,

$$T_{(C,P)} > T_L \tag{5}$$

In the case of malicious, for next round, the child node selects a new parent node. Hence malicious nodes can identify by base station in each round during the decryption of packet. Identified malicious nodes are avoided for route selection. The transmission route is reassessed.

Steps for Removing Malicious Nodes in Network

Step 1: Set up a link in the network of N nodes.

Step 2: Let R = $\{r_1, r_2, \ldots r_k\}$ denote the set of transmission routes.

Step 3: $T_{(C,P)}$ denotes the trust value pair of child parent link.

Step 4: Then the trust value of link is given by $T_{(C,P)} = \{(C_1, P_1), (C_2, P_2) \ldots (C_n, P_n)\}$.

Step 5: (C_1, P_1) be the trust value if first pair in the link, (C_2, P_2) be the next pair link and so on and these value pairs are compared with the network pre-defined threshold value.

Step 6: The threshold value of the network is denoted by T_L.

Step 7: If $T_{(C,P)} = T_L$, link is exists in the network.

Step 8: If $T_{(C,P)} < T_L$, parent node is malicious, else if $T_{(C,P)} > T_L$, child node is malicious.

Step 9: Then the transmission route R is reassessed by changing the nodes.

Apart from the malicious nodes that cause packet losses in the network, we also have to consider the nodes that cause congestion in the network. Congestion detection in intermediate nodes plays important role in congestion control. Nodes are aware of location and its energy levels. Each node should know the probability of sending and receiving the packets before transmission of packets. The consumption of energy is based on the path selection. The degraded link leads to loss of more energy which in turn reduces the network performance.

3. EFFICIENT ENHANCED ROUTE REASSESSMENT ALGORITHM

The proposed algorithm Efficient Enhanced Route Reassessment Algorithm (EERRA) in wireless sensor network achieves the congestion control based on the probability of nodes. The algorithm determines the parent node and route node selection, which eliminates the malicious nodes and low priority nodes in the network, this minimize the congestion and energy consumption.

Each packet from source to base station can flow through multiple paths. Congestion may occur anywhere either from source node or any intermediate nodes. Congestion causes more traffic in the network, and if traffic is increases it causes the network to loss some of the packets. Congestion control helps in preventing the data traffic in network and to achieve the maximum lifetime of network. In this case, intermediate nodes need to identify the congestion nodes or low priority nodes in the network for the effective optimal path selection. In this algorithm, the intermediate nodes keep track of information about the priority of their neighbor nodes. If any congestion is detected in the network, the sending rates of congested nodes that share more bandwidth are limited based on their priority.

In N number of nodes, each child node has priority P_c that shows the data flow generated by that particular source node. Each child node sends the data to parent node which has priority P_s. Every node has certain priorities, then priority of the link is examined by analyzing those probabilities of nodes in the network. Total probability of a pair P_l is calculated which the arithmetic means is of source nodes. Let df be the data flow rate, for every node i, the probability of data flow for child node is

$$P_c(i) = \Sigma_{df \in N} \frac{i(df)}{(df)} P_c(df) \tag{6}$$

Similarly the probability of data flow for parent node is identified by,

$$P_s(i) = \Sigma_{df \in N} \frac{i(df)}{(df)} P_s(df) \tag{7}$$

From the equations (6) & (7), the probability of child and parent link is determined. Total probability of single child parent pair in a network is identified by,

$$P_l = P_c(i) + P_s(i) \tag{8}$$

Similarly this can be applied to all the nodes in the network. This process is repeated for until all child and parent nodes and link priorities are known. The overall probability of link is identified by combining all the child parent node probability of link.

$$P_T = P_{l1} + P_{l2} + \ldots + P_{ln} \tag{9}$$

P_T denotes the total probability of a link that sends and receives the packets. After finding the total probability of link, the capacity of each node is calculated. The nodes which cause congestion are considered as low priority nodes and eliminated and algorithm reassess the path for the effective transmission of data. Nodes which transmit more number of packets are considered for path selection which avoids transmission congestion.

Efficient Enhanced Route Reassessment Algorithm (EERRA) steps are given below:

Step 1: Consider a tree structure that each child node detects their parent node for forwarding the packet towards base station.

Step 2: Child node transmits the packets to parent node which contains the identity information and trust value.

Step 3: All the intermediate nodes keep track of priority of neighbor nodes.

Step 4: The probability of each child node P_c(i) and probability of each parent node P_s(i) is determined.

Step 5: This process is repeated for until all child and parent nodes and link priorities are known.

Step 6: The total probability of link P_l is determined.

Step 7: $P_l = P_c(i) + P_s(i)$ is calculated.

Step 8: The overall probability of link P_T is determined.

Step 9: Low priority nodes are eliminated and route is reassessed.

Step 10: Malicious nodes are identified and removed by base station by comparing the pre-recorded threshold value with all suspicious pair values.

Using efficient enhanced route reassessment algorithm (EERRA) effective path is established based on probability of nodes. If the node does not have the sufficient probability of sending and receiving the packets the alternate node with required probability is selected by algorithm. EERRA discovers a new route if any malicious or low priority nodes in the link. This improves the path stability of network and achieves more number of packet deliveries.

Proposed Packet Format

Packet ID: It comprises details of each and every wireless node. It contains position of node and status updates identification of nodes in network structure.

Source ID	Destination ID	Node Priority Status	Congestion control	Path Stability	Route Reassessment
2	2	4	4	4	2

Figure 2: Proposed Packet format

Figure 2 shows the proposed packet format. Here the source node ID and destination node ID fields take 2 bytes. Third one is node priority status. It indicates whether a node have highest priority or low priority of data transmission. Fourth field is congestion control. These shows the status of link in network is congested or good enough for packet delivery. Fifth field shows the status of path stability of network. The last field indicates the selection of optimal path of network. EERRA algorithm reassesses the path in the presence of any low priority and malicious nodes in link.

IV. PERFORMANCE ANALYSIS

Network Simulator NS-2.34 version is used to simulate proposed Efficient Enhanced Route Reassessment Algorithm (EERRA). NS-2 is an object oriented tool command language. It supports to simulate various

networks Technologies WSN, VANET, and MANET. NS-2.34 is based C++ language; ease of code, and implements a lot of protocol designs.

In our simulation, 100 sensor nodes move around a 1000 meter x 1000 meter square region for 15 milliseconds simulation time. All nodes have the equal coverage range of 250 meters. Mac address 802.11 is inbuilt in design and the simulation setting and parameters are summarized in table.

Table 1
Simulation setup of proposed protocol

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Simulation Time	15ms
Radio Range	250m
Traffic Source	CBR
Packet Size	512 bytes
Mobility	Random Way Point
Protocol	LEACH protocol

Simulation Result: Figure 3 shows that the proposed method Efficient Enhanced Route Reassessment Algorithm (EERRA) is an efficient one compared with existing NBMND [3] and TR-SDTN [8]. It enhances security to detect bad mouthing attack occurred in network, and also reduce the congestion during transmission by picking the optimal path.

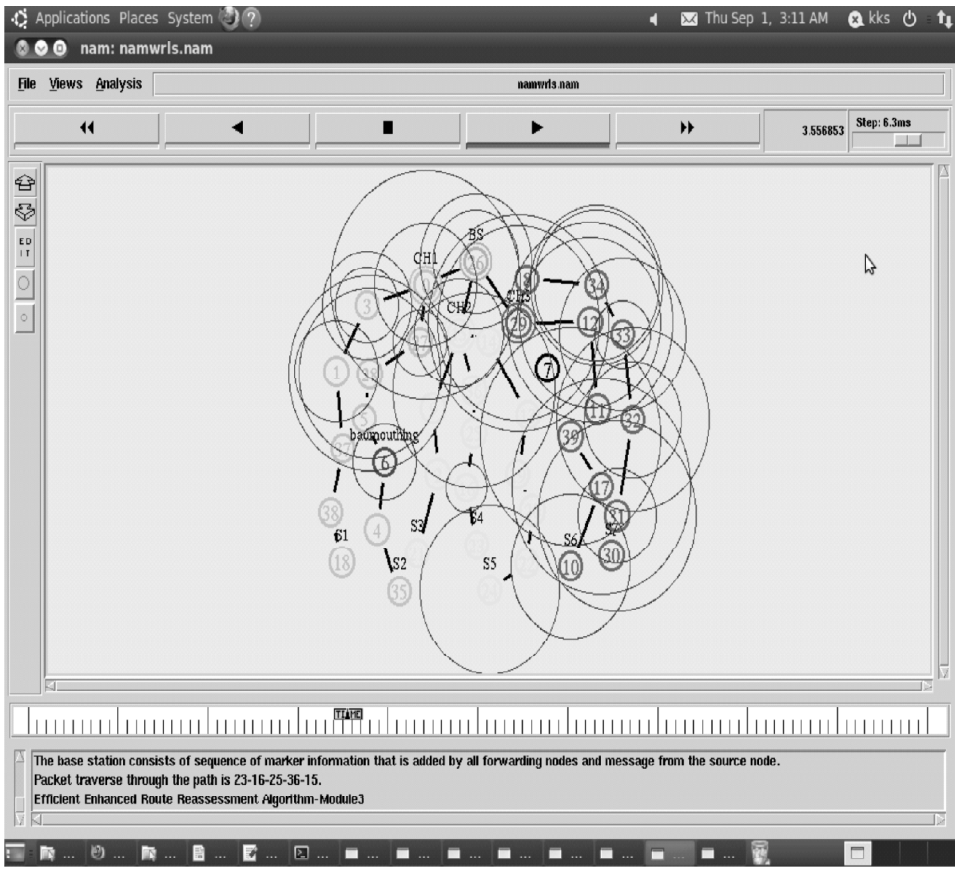

Figure 3: Proposed EERRA Result

Performance Analysis

X-graph is used in simulation to examine the following performance metrics in ns2.34.

Packet Delivery Ratio: Figure 4 shows packet delivery ratio which is measured by number of received packets from number of forwarded packets in particular speed. Fixed speed in simulation is 100(bps). In proposed EERRA method packet delivery ratio is increased compared to existing methods HBRP, SICRA, TR-SDTN, NBMND.

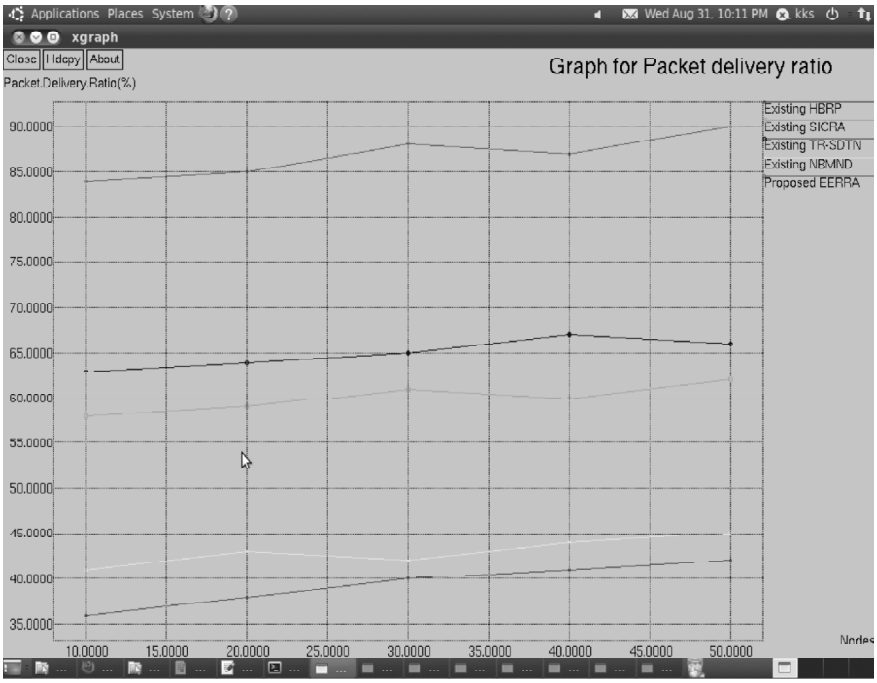

Figure 4: Graph for No. of Nodes Vs. Packet Delivery Ratio

Network overhead: Figure 5 shows rate of network overhead occurs during packet transfer for entire transmission from source node to root node. This shows load balancing in network. In proposed EERRA method network overhead is decreased compared to existing methods HBRP, SICRA, TR-SDTN, NBMND.

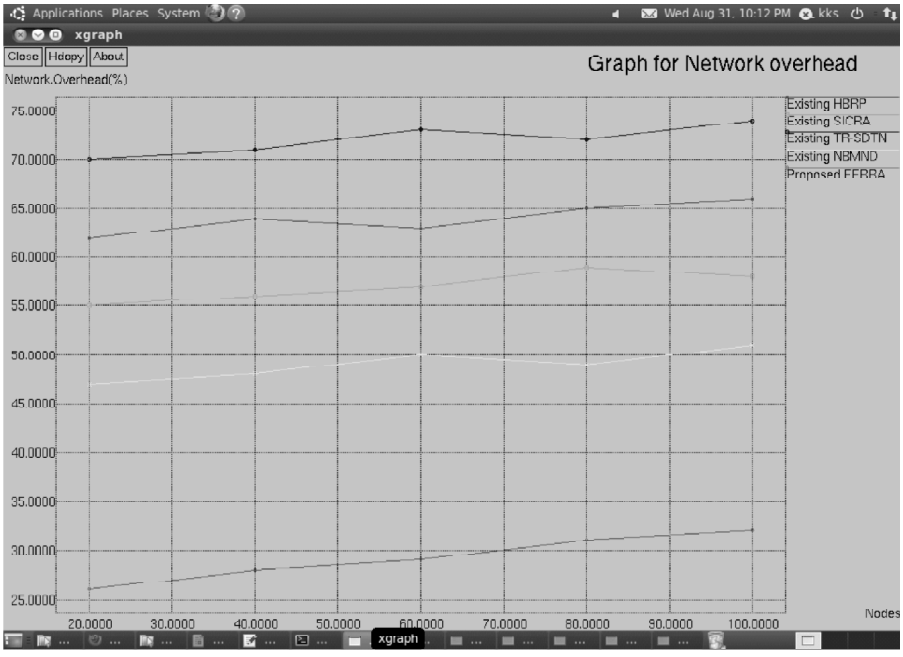

Figure 5: Graph for No. of Nodes Vs. Network overhead

Packet Loss Rate: Packet loss occurs when nodes fail to send the packets to receiver node based on insufficient capacity of node in a network. Figure 6 shows packet loss ratio that occurs during transmission between sender nodes to route path In proposed EERRA method Packet loss rate is minimized compared to existing methods HBRP, SICRA, TR-SDTN, NBMND.

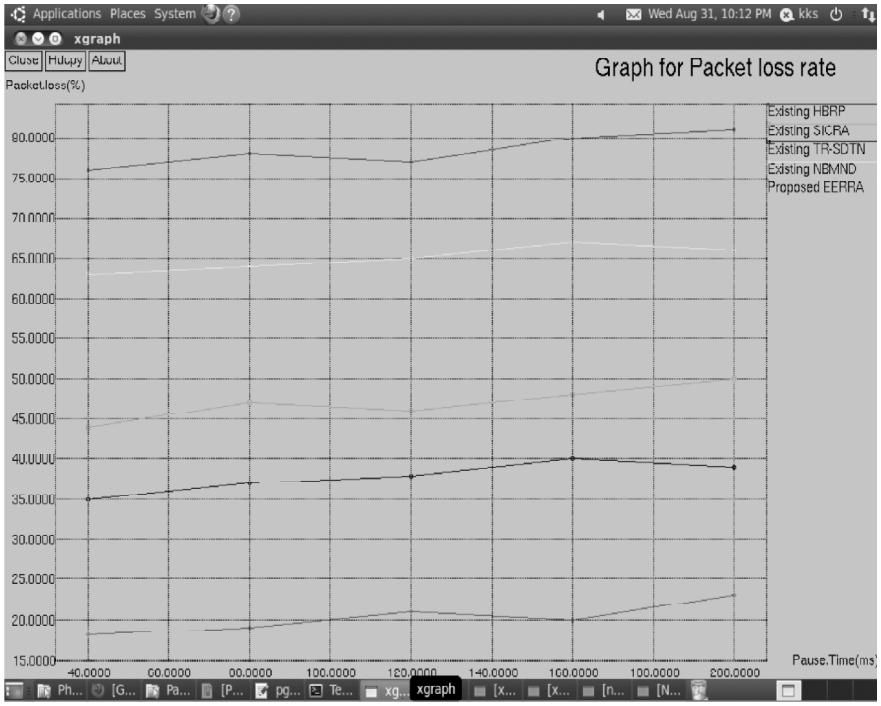

Figure 6: Graph for Time Vs. Packet loss

Network Lifetime: Figure 7 shows the lifetime of network. The lifetime of network is the time to the failure of first sensor node. In Proposed EERRA method the network lifetime is improved compared to existing methods HBRP, SICRA, TR-SDTN, NBMND.

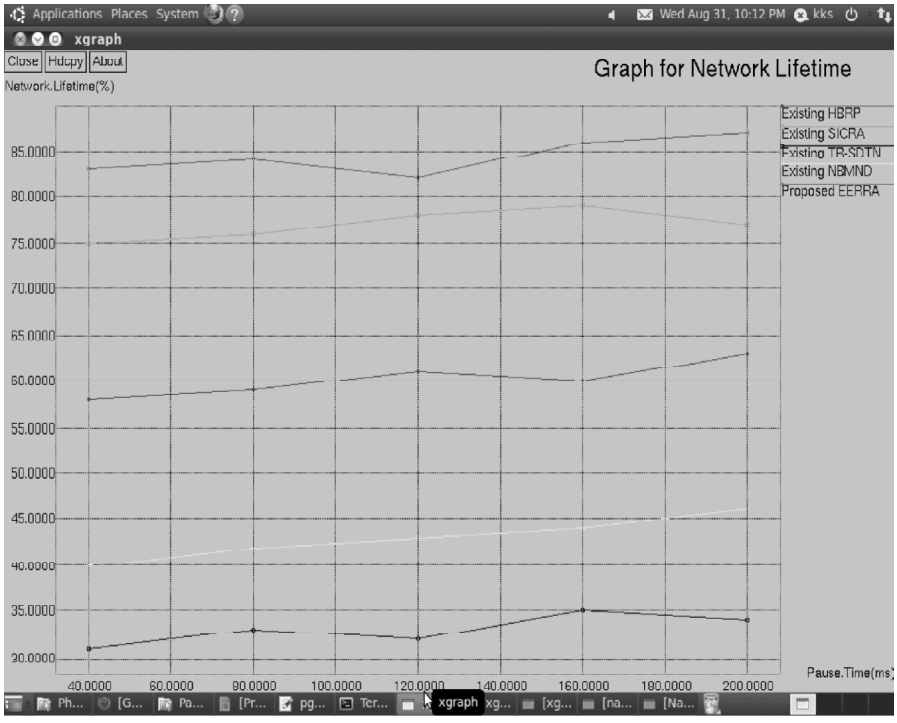

Figure 7: Graph for Time Vs. Network Lifetime

Path Stability: Figure 8 shows the path stability of sensor network. It evaluates the network stability. Path stability level has straight relation to number of updates to preserve accurate view of network state. In proposed EERRA method the path is more stable compared to the existing methods HBRP, SICRA, TR-SDTN, and NBMND.

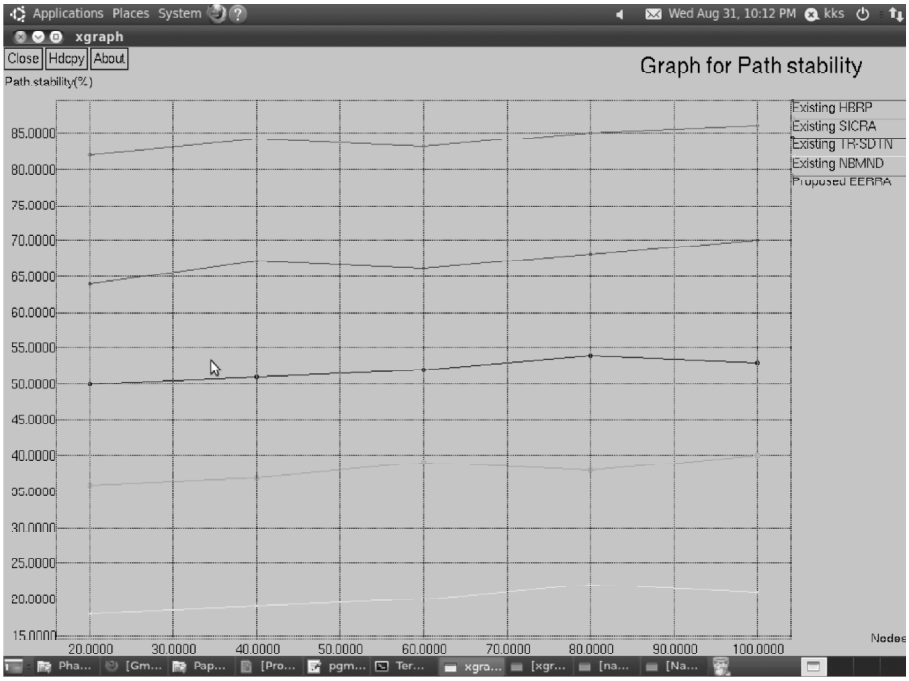

Figure 8: Graph for No. of Nodes Vs. Path Stability

Energy Consumption: Figure 9 shows energy consumption that is how much energy consume for particular packet transmission, calculates consumption of energy from initial energy level to final energy level. In proposed EERRA method energy consumption is reduced compared to existing methods HBRP, SICRA, TR-SDTN, and NBMND.

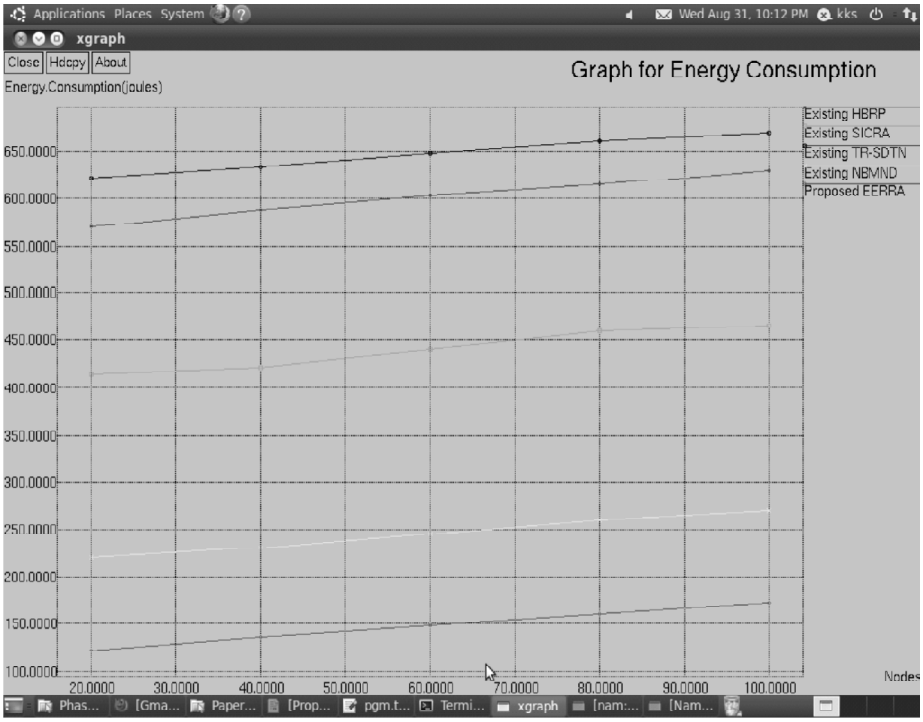

Figure 9: Graph for No. of Nodes Vs. Energy Consumption

V. CONCLUSION

In wireless sensor network, the presence of compromised nodes and malicious nodes cause the poor performance of data transmission. The proposed Efficient Enhanced Route Reassessment Algorithm (EERRA) effectively detects and eliminates the low priority nodes from the link and selects optimal path. The proposed work monitors for the bad mouthing attack. The faulty nodes are identified by comparing the trust value of suspicious pair with the network predefined threshold value. This process is carried out during decryption of packet by base station. In this case the algorithm reassesses the path by picking another node with sufficient probability to transmit the packets. Every node keeps track of neighbor node priority in order to avoid the congestion in network, low priority nodes are removed from the link. This prevents the congestion and loss of packets in network link and improves the path stability. It enables the route assessment is conducted flexibly and it reduces the congestion to a greater extent. The simulation results of NS2 shows that the proposed algorithm picks the optimal path that improves the path stability and network lifetime. The performance analysis of EERRA increases packet delivery ratio and minimize the packet loss, energy consumption and network overhead than the existing HBRP and SICRA.

References

[1] Jan, Roohullah. "Congestion Control in Wireless Sensor Networks-An overview of Current Trends."

[2] Noori, Moslem, and Masoud Ardakani. "A probability model for lifetime of wireless sensor networks." arXiv preprint arXiv:0710.0020 (2007).

[3] Yim, Sung-Jib, and Yoon-Hwa Choi. "Neighbor-based malicious node detection in wireless sensor networks." (2012).

[4] Mori, Shintaro. "Cooperative sensing data collecting framework by using unmanned aircraft vehicle in wireless sensor network." 2016 IEEE International Conference on Communications (ICC). IEEE, 2016.

[5] Tian, Ying, *et al.* "A node schedule method for multi-coverage probability based on probabilistic coverage in WSNs." 2016 Chinese Control and Decision Conference (CCDC). IEEE, 2016.

[6] Alanazi, Adwan, and Khaled Elleithy. "Optimized Node Selection Process for quality of service provisioning over wireless multimedia sensor networks." 2016 Second International Conference on Mobile and Secure Services (MobiSecServ). IEEE, 2016.

[7] Gallegos, Alberto, *et al.* "Simulation study of Maximum Amount Shortest Path routing in Wireless Sensor Networks using Ns-3." 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2016.

[8] Zhang, Zhenjing, Maode Ma, and Zhigang Jin. "TR-SDTN: Trust based efficient routing in hostile social DTNs." 2015 IEEE International Conference on Communication Workshop (ICCW). IEEE, 2015.

[9] Shabut, Antesar M., *et al.* "Recommendation based trust model with an effective defence scheme for MANETs." IEEE Transactions on Mobile Computing 14.10 (2015): 2101-2115.

[10] Wu, Jiajing, K. Tse Chi, and Francis CM Lau. "Concept of Node Usage Probability From Complex Networks and Its Applications to Communication Network Design." IEEE Transactions on Circuits and Systems I: Regular Papers 62.4 (2015): 1195-1204.

[11] Ahmed, Gulnaz, *et al.* "Analyzing algorithms in Wireless Body Area Sensor Networks: A survey."2015 Fourth International Conference on Aerospace Science and Engineering (ICASE). IEEE, 2015.

[12] Suh, Bongsue, and Stevan Berber. "Rendezvous points and routing path-selection strategies for wireless sensor networks with mobile sink."Electronics Letters 52.2 (2015): 167-169.

[13] Jamil, Saima, *et al.* "COPE: Cooperative Power and Energy-efficient routing protocol for Wireless Sensor Networks." Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on. IEEE, 2015.

[14] Khedim, Farah, Nabila Labraoui, and Mohamed Lehsaini. "Dishonest recommendation attacks in wireless sensor networks: A survey."Programming and Systems (ISPS), 2015 12th International Symposium on. IEEE, 2015.

[15] Islam, M. Hasan, and Adnan Ahmed Khan. "Detection of dishonest trust recommendations in mobile ad hoc networks." Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on. IEEE, 2014.

[16] Gao, Cai, *et al.* "A bio-inspired algorithm for route selection in wireless sensor networks." IEEE Communications Letters 18.11 (2014): 2019-2022.

[17] Anuradha, M. P., and Gopinath Ganapathy. "Data Aggregation Using Probability Theory For Wireless Sensor Networks."

[18] Oh, Seo Hyun, Chan O. Hong, and Yoon Hwa Choi. "A malicious and malfunctioning node detection scheme for wireless sensor networks."Wireless sensor network 4.03 (2012): 84.

[19] He, Xin, Xiaolin Gui, and Wei Wei. "A heider-theory based reputation framework for wsn." High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on. IEEE, 2008.

[20] Mingwu, Zhang, *et al.* "Using trust metric to detect malicious behaviors in WSNs." Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on. Vol. 3. IEEE, 2007.

[21] Li, Zhibin, and Peter X. Liu. "Priority-based congestion control in multi-path and multi-hop wireless sensor networks." Robotics and Biomimetics, 2007. ROBIO 2007. IEEE International Conference on. IEEE, 2007.

[22] Curiac, Daniel-Ioan, *et al.* "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique." ICNS 7 (2007): 83-88.

[23] Agarwal, Richa, and Amit Kumar Gautam. "A Probability based Energy Efficient Clustering Protocol in Wireless Sensor Network."