A Framework for Event Anomaly Detection in Cognitive Radio Based Smart Community

S. M. Nadim Uddin*, Nafees Mansoor†, Musfiqur Rahman‡, Nabeel Mohammed§ and Sazzad Hossain¶
*‡ Department of Electronics and Telecommunication Engineering, University of Liberal Arts Bangladesh.
†§¶ Department of Computer Science and Engineering,University of Liberal Arts Bangladesh.
Email:*sm.uddin.ete@ulab.edu.bd, †nafees.mansoor@ulab.edu.bd ‡musfiqur.rahman.ete@ulab.edu.bd§nabeel.mohammed@ulab.edu.bd
¶sazzad.hossain@ulab.edu.bd

***Abstract*—With the advancement of technology, a surge of research interest in cognitive radio based networks in smart communities has been mounting. It is anticipated that CR-enabled networks will play a vigorous role in the enrichment of communication efficiency in neighborhood sensor area network. This paper presents a framework for Cognitive Radio based event anomaly detection mechanism. A skeleton for intelligent learning, detection and decision mechanism for Local Controller Unit and a Primary Controller Unit is also proposed and discussed in the model. The proposed model has four distinct layers namely sensors, routers, Local Controller Unit and Primary Controller Unit. A scheme for emergency situation detection and notification has been proposed. This paper also introduces a cluster formation scheme for better accuracy in data transmission among different hierarchical layers. The network module of the proposed model is later simulated and validated for some important performance communication metrics.**

***Keywords*—Cognitive radio, Neighborhood area network, WSN, Anomaly detection.**

I. Introduction

With the development of the communication technology and microelectronic devices, a surge of interest in designing smart networks based on cognitive radio mechanism for smart communities has been increasing among academics as well as researchers. Neighborhood Sensor Area Network (NSAN) is a variation of the Neighborhood Area Network (NAN) in smart community and consists of the communications of smart router units and sensors with a back-end local control center. Though adopting wireless mesh topology can be a suitable solution for efficient communication, to overcome the network congestion problem and the growing demand of radio spectrum, proper utilization of the radio spectrum is essential[1]. Cognitive radio enables dynamic spectrum allocation technique to utilize radio spectrum efficiently [1][2][3].

However, data delivery in sensor networks is faulty and unpredictable [4], which lead to data anomaly. Anomaly refers to the problem of recognizing patterns in data that do not conform to expected behavior [5]. Anomaly detection in sensor networks poses a set of unique challenges. A sensor network comprises of sensors that collect different types of data, such as binary, discrete, continuous etc. Failures in wireless sensor networks can occur for various reasons due to fragility, depletion of batteries or destruction by an external event. In addition, nodes may capture and communicate incorrect readings because of environmental influence on their sensing components. Moreover, links in any ad hoc wireless networks are failure-prone [6], causing network partitions and dynamic changes in network topology. Additionally, the anomaly detection techniques need to be light- weight and in a distributed fashion due to resource constraints [5].

For the past few years, different anomaly detection approaches have been proposed to improve communication in wireless networks. Most of these techniques use the machine learning and statistical approaches for anomaly detection [7]. Moreover, these techniques can be categorized into three groups, namely unsupervised clustering, semi-supervised classification and supervised classification. Comparing with the other two groups, clustering approaches exhibit higher reliability in communication [8]. However, communication networks for smart grids also require to consider additional parameters, such as, application requirements, link capacity, traffic settings, cost, scalability, etc. [9][10]. It is also observed that very little considerations have been made for anomaly detection in cognitive radio oriented smart community. Thus, anomaly detection in this area remains to be at the infant stage.

In this paper, a framework for cognitive radio based anomaly detection mechanism in smart communities has been proposed. A conceptual architecture with a wireless hybrid topology has been proposed to integrate sensing, computation and decision-making for enabling efficient detection of anomaly. In the proposed model, two distinct types of anomaly detection mechanism using Exponentially Weighted Moving Average and Anomaly factor based on Brier's Score are proposed. The remainder of this paper is organized as follows. Section II demonstrates the abstract and deployment view of the proposed framework. In Section III, simulations results are presented and discussed. The paper ends with Section IV, where this section presents conclusion and future works.

II. Proposed Framework

A. System architecture

The proposed model consists of five levels of hierarchy namely sensors, routers, local controller unit (LCU), Database layer and primary controller unit (PCU). The first layer of the architecture is composed of hundreds of sensors situated in the street areas are grouped into clusters, sending their data

directly to routers. Sensors are assumed to be dispersed in a 2 dimensional space and are quasi-stationary. Sensors transmit at the same fixed power levels, which is dependent on the transmission distance. It is assumed that the energy consumption among nodes is not uniform. The routers, the second layer of the architecture, are responsible for transmitting the received data to the LCU. The third layer is LCU, a test and control unit that is responsible for applying control over the routers and sensors. Routers and the LCUs are connected via wireless mesh network in a multi-hop manner. The forth layer is the Database layer that will store the aggregated data received from layers below, and feed the PCU with collected data. PCU and the LCUs keep databases of unusual behaviors of different devices at different levels of the hierarchy. The databases are used to predict damages or determine emergency situation levels.

In the proposed model, each node at a level of the hierarchy sends control message to the node of upper level or among themselves. The control message is used for connection set up, cluster formation, message delivery completion, instantaneous data fetch command, etc. Information messages transmitted and received among nodes are defined as sensed data from the terminal sensor devices, combined data from Nodes to routers, combined data from routers to LCU and Filtered and combined data from LCUs to PCU. A Primary Controller Unit (PCU) is proposed to be placed in the network for data storage, processing and decision making. It is the top layer and applies control over the entire neighborhood area. It accesses sensing units directly in emergency situations, or indirectly through the DB layer in normal conditions.

Data packet, in the model, follows a basic structure consisting of sender node id, information, destination id, hop count, timer, sequence number etc. The routing path for source to destination is determined by the greedy forwarding algorithm.

B. Network model

Each grid is proposed to be hexagonal in shape and is divided into six sub-grids. The proposed environment is a mesh network in which the LCU is located at the center of the grid to make LCU-router and LCU-LCU communication easier. According to the proposed model, one LCU can serve six sub-grids and is efficient for installation costs and maintenance. The topology ensures equidistant LCUs in a community. The connection between the router and the terminal sensor nodes is set by a control message sent by the router. Upon reception of the message by the sensor node, an acknowledgement message is sent to the router and connection is established. This process continues until all nodes of different clusters are connected to the router. The router collects the data from the cluster of nodes, verifies and uploads the data to the LCU. Unable to connect, the router waits for a threshold time and tries again. After trying for a threshold number of attempt, the router takes a log of the nodes along with the associated data and sends notification to the LCU and waits for instructions. The connection establishment mechanism between LCU and router is similar to the connection between the sensors and router. LCU receives data from the router and analyses data of that router. If the data complies with the database, LCU keeps the data for threshold time and then rejects it. If the data varies from the threshold, LCU finds out the problem node or the cluster. Appropriate commands from the database are selected and sent it to routers as a counter-measure. If appropriate commands are not found in LCU's database for a specific event, a control message along with the data is sent to PCU for analysis and counter-measure. PCU receives information data from the LCUs in a community. Depending on the variance of the data, it sends command to LCU or put the system into a warning state. Figure 1 illustrates the hierarchical data processing of the proposed model.

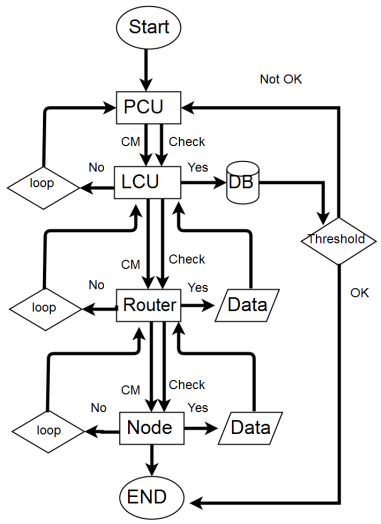

Fig. 1: Flow chart of data movement in the proposed network.

C. Detection mechanism

In the sensor receiver, the returning signal comprises the wanted data and the unwanted niose. The router determines whether point anomaly has occurred in nodes i.e. an individual data instance that can be considered as anomalous with respect to the rest of data. To determine point anomaly, router calculates the Exponentially Weighted Moving Average (EWMA) of each nodes which acts as the baseline or the reference model for each node. Let $\Theta \leq 1$ denote a constant and ζ_t is the mean of data value at time t, the Exponentially Weighted Moving Average (EWMA) [11] of a node Γ_t is,

$$\Gamma_t = \Theta\zeta + (1 - \Theta)\Gamma_{t-1} \tag{1}$$

The EWMA value changes with time as it depends on the previous value. However, if the data value of a node crosses EWMA by a threshold value, the router recognizes the event as important and sends command to LCU for further instruction. Figure 2 illustrates a basic detection of point anomaly of a node.

LCU maintains network through techniques that operate in a semi- supervised mode and it is assumed that the training data has been labeled for instances for only the normal class.

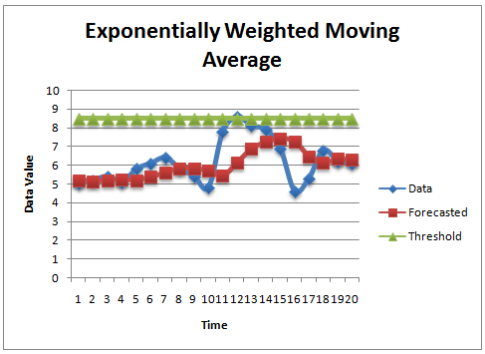

Fig. 2: Detection of point anomaly.

The LCU checks if a collection of related data instances from routers is anomalous with respect to the entire data set. If so, it marks it as a collective anomaly and checks for problem node or router in divide and conquer manner i.e. going through each division of the router. On each division, based on [12], LCU uses hyper-ellipsoids for k dimensional inputs for calculating Radial Basis Function for the Multi Layer Parametric approach in case of data classification. .

Let w_{jk} be the vector of weights of the node from the LCU, $\Phi(.)$ be the activation function and $||x-\mu_j||$ be the Euclidean distance, then the Response Function of system, τ_k can be defined as,

$$\tau_k = \sum_{j=1}^{m} w_{jk} \Phi \left(\frac{\|x-\mu_j\|}{\sigma_j} \right) \tag{2}$$

where m $\in N$ is the number of nodes where N is the set of natural numbers, $\mu_j(x)$ is the centroid of the network and σ_j is the smoothing factors which may vary depending on the distance.

The activation function which shapes the network system is selected to be Gaussian Radial Basis Function (RBF). Let d be the dimension of data from an input and $\sigma_j^2(x)$ be the variance, then the RBF, Φ can be defined as,

$$\Phi(t|x) = \frac{1}{[2\pi]^{\frac{d}{2}} \sigma_j^k(x)} e^{-\frac{\|t-\mu(x)\|^2}{2\sigma_j^2(x)}} \tag{3}$$

For generality, it is assumed that the smoothing factors σ_j are equal for all nodes. Based on validation, LCU assigns an anomaly factor for each router through which anomaly can be detected. Inspired from Brier's Score, the factor δ can be expressed as,

$$\delta = \frac{1}{N} \sum_{t=1}^{N} (\alpha_t - \beta_t)^2 \tag{4}$$

Where α_t is the category of the anomaly, β_t is the outcome of the observation at time t and N is the total observation. Depending on the variance of the output, LCU decides commands from the database or sends data to PCU. During warning state, an emergency protocol command from PCU is carried out to routers via LCU to monitor specific regions. In such case, a new cluster of nodes is formed to focus on a specific region and the nodes can bypass normal procedures and directly send data to other routers and LCUs for accuracy and effective data transmission. In emergency situations, each node in every level is capable of sending some emergency messages to other nodes. This type of message includes instantaneous information of node, connection hierarchy bypass message, power messages which include emergency shutdown, emergency network buildup, system restoration messages etc. PCU retrieves data from that region more frequently and calculates the data variations. Depending on the variation of data, the PCU turns off the state, puts the system on halt or sends alarm to house owners and local authority and stores the data in database for future decisions.

D. Cluster formation

The proposed clustering mechanism is inspired from the clustering scheme for cognitive radio ad-hoc network in [3]. In the existing clustering mechanism, cluster-head selection is based upon a parameter called cluster-head determining factor (CHDF) where CHDF of a node is calculated over number of common channels and number of neighboring nodes.

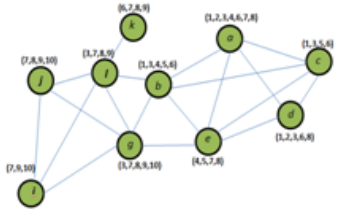

Fig. 3: Connectivity graph of a CRN with the accessible channels' sets in the brackets.

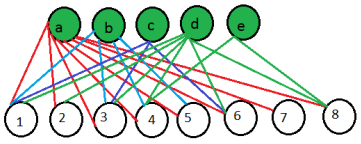

Fig. 4: Bipartite graph constructed by node.

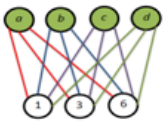

Fig. 5: Maximum edge biclique graph of node.

The proposed cluster formation stage starts once nodes in the network finish the neighbor discovery process. Next, the nodes share accessible channel lists (ACLs) C_i and neighbors list N_i among 1-hop neighbors (where i = 1, 2, 3 n). The

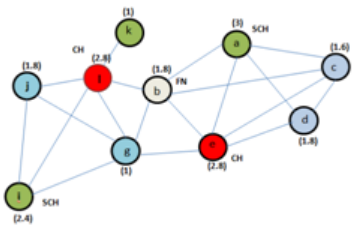

Fig. 6: Cluster-head, Secondary Cluster-head and Cluster Member selection.

proposed clustering scheme is defined as a maximum edge biclique problem. Based on neighbor list N_i and accessible channels list C_i, each CR_i constructs an undirected bipartite graph G_i (A_i, B_i, E_i). Here, A_i = $CR_i \cup N_i$, and B_i= C_i. An edge (x, y) exists between vertices x $\in$ A_i and y $\in$ B_i if y $\in$ C_i, i.e., channel y is in the channel list of CR_i. From the bipartite graph, each node in the network constructs its own maximum edge biclique graph. From the maximum edge biclique graph, node determines new C_i and N_i values. The proposed clustering scheme aims to allocate maximum number of free common channels per cluster with suitable amount of member nodes. A parameter called Cluster Head Determination Factor (CHDF) is used to select cluster heads. Every CR calculates CHDF based on equation (5).

$$CHDF = \sqrt[C_i]{{C_i}^{N_i}}; i = 1, 2, 3, \ldots \quad (5)$$

Where, C_i is number of free common channels and N_i is the number of neighboring nodes of CR_i. A node declares itself as cluster head if its own CHDF value is higher than all its neighbors. Once the CHDF value of a node CR_i is lesser than any of its neighbor, CR_i joins the neighboring node that has the highest value as cluster member (CM). After the cluster formation, CH selects SCH from the CMs based on the CHDF value. The SCH takes charge of the cluster if current CH moves out, which shrinks the possibility of re-clustering.

III. Simulation and Results

A. Simulation setup

To simulate and analyze performances namely throughput, delay and routing overhead of the proposed network model for the proposed network model, discrete-event simulator NS2 has been used and the performance analysis are conducted using PERL scripts.

A simulation area of 10000 m^3 is considered for the simulation purpose. Drop-tail method is used for the queuing purpose. IEEE 802.11 is considered as the MAC type and TCP is considered for Transport Layer. Maximum packet queuing delay is considered as 50 μs. In the simulation, AODV is used as the routing protocol while data traffic is generated with Constant Bit Rate (CBR) with packet size is set to 512 bytes. Varied packet rate ranging from 100 packets/sec to 800 packets/sec is considered to evaluate the performance of the network for different traffic load. The number of nodes is considered to be 100. Initial energy for all nodes is considered to be 100 Joules. The simulations are run for 240s each.

B. Evaluation

This section of the paper discusses the simulation results of the proposed model in terms of throughput, energy consumption, delay and overhead.

1) Performance based on Throughput: In this paper, throughput is defined as the number of successfully received data packets at the destination node in a unit time and it is represented in Kbps.

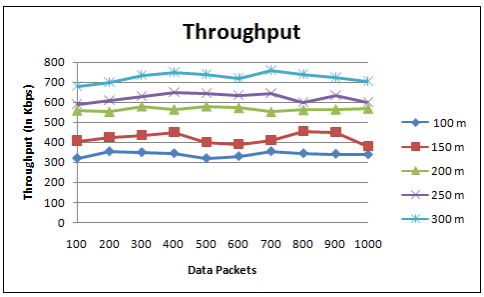

Fig. 7: Throughput for the proposed network.

Figure 7 shows that with an increasing traffic load, throughput for all scenarios increases. However, throughput is higher in the network with the longer radio transmission range, than the other radio transmission ranges for all different data flow rates. This is because; a network with longer ranged transmission finds lesser number of hops to transmit packets to the destination. Thus, with decreasing number of hops, number of links throughout the network, probability of link failure and rate of packet retransmission reduce significantly. Therefore, with higher transmission range, throughput of the network increases for all different traffic loads.

2) Performance based on Packet Delivery Ratio: In this paper, the packet transmission delay is defined as the average time required for transferring data packets from the source node to the destination node. Packet delivery ratio is expressed in percentage.

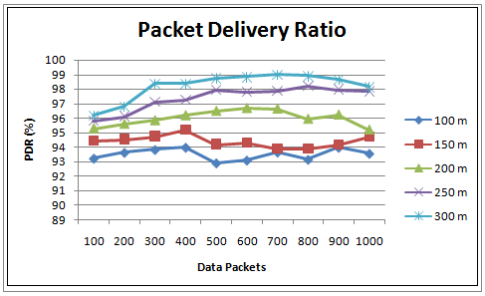

Fig. 8: Packet delivery ratio for the proposed network.

From the figure, it is observed that the packet transmission delay increases with increasing data flow rate in both scenarios because when traffic load is increased, more data packets need to be transmitted from the source to the destination node. As

a result, the intermediate nodes are required to process more packets which eventually increases individual data processing sessions among the nodes. Thus, when higher number of packets propagates, source node and the intermediate nodes need longer time to forward the packets to the next hop, which increases the cumulative packet transmission delay. Moreover, lesser number of intermediate nodes is engaged to forward the data in long transmission ranged network, which results lesser data processing sessions. Therefore, a network with long transmission ranged radios results lesser packet transmission delay than that of a network with short transmission ranged radios.

3) Performance based on Overhead Ratio: The network overhead is defined as the total transmitted control packets over total received data packet at the destination node.

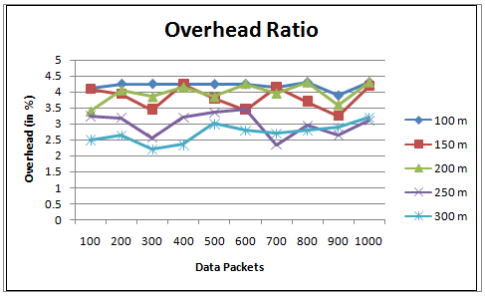

Fig. 9: Overhead ratio for the proposed network.

From the figure, it is seen that the overhead ratio increases with increasing data flow rate in both scenarios. Increase in data rate means nodes need to process more data packets individually which eventually results in reduction of a node's efficiency for packet forwarding. It is also observed from Fig. 7 that the overhead ratio is lesser in a network with longer radio transmission ranged network compared to the network with shorter radio transmission ranged network for all different traffic loads. That is because, in a shorter radio transmission ranged network, more nodes will have to process increased traffic load and as a result, retransmission of data packets due to exceeding node's capacity to process data packets will increase which eventually increases number of transmitted control packets.

IV. Conclusion

In this paper, a framework for cognitive radio based event anomaly detection mechanism in neighborhood sensor area network has been proposed. A concept of adapting exponentially weighted moving average for point anomaly and anomaly factor for cumulative anomaly has been outlined and a clustering scheme for emergency situations has been proposed. The next research project will involve designing a robust algorithm for labeling anomalies and system optimization as well situation handling mechanism.

References

[1] W. Saad, Z. Han, A. Hjorungnes, D. Niyato, and E. Hossain, "Coalition formation games for distributed cooperation among roadside units in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 48–60, 2011.

[2] N. Mansoor, A. M. Islam, M. Zareei, S. Baharun, T. Wakabayashi, and S. Komaki, "Cognitive radio ad-hoc network architectures: a survey," *Wireless Personal Communications*, vol. 81, no. 3, pp. 1117–1142, 2015.

[3] N. Mansoor, A. M. Islam, M. Zareei, S. Baharun, and S. Komaki, "Spectrum aware cluster-based architecture for cognitive radio ad-hoc networks," in *Advances in Electrical Engineering (ICAEE), 2013 International Conference on*. IEEE, 2013, pp. 181–185.

[4] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*. ACM, 2003, pp. 1–13.

[5] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[6] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*. ACM, 2003, pp. 14–27.

[7] M. Markou and S. Singh, "Novelty detection: a reviewpart 1: statistical approaches," *Signal processing*, vol. 83, no. 12, pp. 2481–2497, 2003.

[8] A. L. Dos Santos, E. P. Duarte Jr, and G. M. Keeni, "Reliable distributed network management by replication," *Journal of Network and Systems Management*, vol. 12, no. 2, pp. 191–213, 2004.

[9] Z. Zhu, S. Lambotharan, W. H. Chin, and Z. Fan, "Overview of demand management in smart grid and enabling wireless communication technologies," *IEEE Wireless Communications*, vol. 19, no. 3, pp. 48–56, 2012.

[10] Y. Dong, Z. Cai, M. Yu, and M. Sturer, "Modeling and simulation of the communication networks in smart grid," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 2658–2663.

[11] J. M. Lucas and M. S. Saccucci, "Exponentially weighted moving average control schemes: properties and enhancements," *Technometrics*, vol. 32, no. 1, pp. 1–12, 1990.

[12] T. Brotherton, T. Johnson, and G. Chadderdon, "Classification and novelty detection using linear models and a class dependent-elliptical basis function neural network," in *Neural Networks Proceedings, 1998. IEEE World Congress on Computational Intelligence. The 1998 IEEE International Joint Conference on*, vol. 2. IEEE, 1998, pp. 876–879.