JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Malicious node Detectionand Avoidance in IOT Smart home system by Considering QoS

B.R. Susheel Kumar[1*], **Arun Biradar**[2]

[1,2]Department of CSE, East West Institute of Technology, Bangalore, India

DOI: https://doi.org/10.26438/ijcse/v7si15.388393 | Available online at: www.ijcseonline.org

***Abstract*—**IOT Smart home system is becoming common now a days. In this ecosystem if a data packets are corrupted or manipulated by a faulty or compromised node, then detecting the faulty node is difficult because of multi hop mesh like network. The faulty Node might lead to wrong decision and operation failure of system thus impacting the Quality of Service (QoS) of different client devices. In this paper we first create a smart home ecosystem by usingIOT nodes like Raspberry pi and Node MCU models. We apply unsupervised learning technique on statistical data collected from these nodes to accurately detect faulty/Malicious nodes. We also provide alternate route depending up on the QoS of client device.

***Keywords*—**IOT, Node MCU, Raspberry pi, smart home, unsupervised learning, QoS

I. Introduction

The IOT Smart home system (IoTSHS) extends computing capability to wireless identifiable objects, sensors and sensor embedded smart tiny devices. These deviceswill generate, exchange and consume data with minimal human intervention. These IoTSHS nodes and clients form a distributed mesh network and provide a coverage to entire home [1][2]. Nodes provide connectivity to client devices and data traffic is transported through mesh backhaul to Internet. As many devices will be connected to internetvia the IoTSHS. An offender could attack weakest of them and use this device to infiltrate the entire system. This could serve as endangered entry point for different cyber-attacks such as interception, eavesdropping and modification of confidential information. Depending on the intentions of attackers, devices has different level of risk to be the target of an attack.

The key issue of high security breach owing to internal attacks launched by compromised, yet authenticated node remains a critical point of concern (e.g., Mirai malware [3], Stuxnet attack [4]). These attacks done by compromised nodes could not be intercepted by traditional cryptographic methods [5]. Packet manipulation attack is amongst the most challenging internal threats because of the multi hop mesh like IoTSHS environment. The faulty nodes even consume network resource by having network element transmitting/forwarding corrupted data.

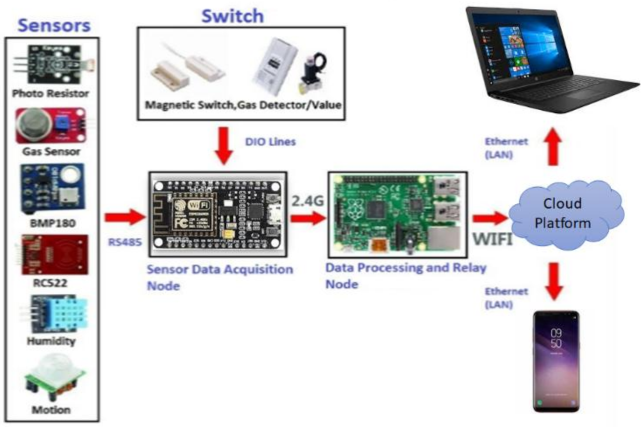


Figure 1.IoTSHS System using Raspberry Pi and Node MCU

There are variouspractical approaches to solve the malicious node detection problem.Inthis paper we choose unsupervised learning mechanism to detect malicious node and alsofocus on providing optimal alternative path for client device based on Quality of Service (QoS), Since the user is more concerned with the detection and recovery from the attacks. The high priority devices should not miss the critical data transmission. For instance, in a mesh like IoTSHS if security cameras detect an intruder, but the devices might disconnect from the network connectivity because of a malicious intermediate node. Thus, the optimal alternative path for QoS critical data plays a major role in recovery from the attacks. For finding optimal path for QoS data we consider the client statistics like bandwidth requirement, location, traffic and usage pattern for over a period. As each user has his own set of high priority clients and these client device statistics varies based on different home environment, we need Artificial

Intelligence (AI) or Machine Learning (ML) techniques to come up with a user or traffic pattern.

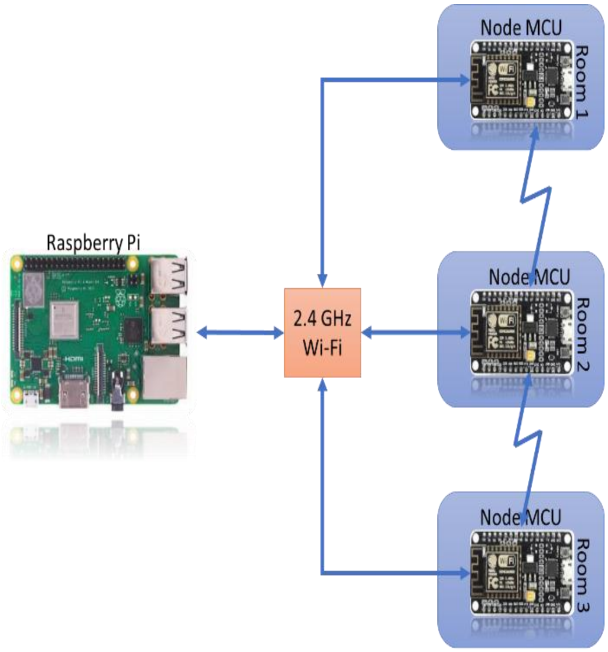


Figure 2.Raspberry Pi and Node MCU in Mesh topology

The rest of paper is organized as follows; related work is covered in section II. In section III we create a multi hop IoTSHS system by using Raspberry pi3 and Node MCU models. Using this IoTSHS we simulate the fault/malicious node detection and provide alternate route based on QOS. Section IVhas results and discussion of the outcome which is followed by Conclusion and future work in section V.

II. Related Work

There are several schemes to detect a malicious node, A watchdog scheme used in [7] where in every node overhear packets forwarded by neighboring nodes and according verify the packet drop. There are schemes were encryption is required in each node for both packet forwarding and generating [6] but these require extra computational and memory resource in each node.

In [8] An en-route filtering scheme to filter false data injected by malicious node is used but this fails to detect malicious nodes. In [9] hard fusion rule is used in a centralized communication environment which might not available in many IoTSHS.There are trusted nodes schemes used to detect single hop errors [10]. And in multi hop mesh network they depend on network diversity to detect a malicious node but both these schemesrequire large overhead information to be added to each packet [11][12].

Even various Machine learning schemes are used in detecting a malicious node, in [13]one class support vector machine (SVM) assisted by Fisher Discriminant Analysis technique [14] are used to find the malicious behavior by using bandwidth and hop count as training set yet they fail in finding malicious node.

Neural network technique with certain sensor confidence factor defined [15], and also Bayesian Belief network [16] is used to predict sensor data.By taking the difference between the actual data and predicted data a certain node can be classified as faulty/malicious node but here they depend on the reliable data transfer to central unit, which cannot be assured if some nodes are compromised.

Supervised Machine learning schemes have some limitations since its expensive to train a data set [17] and there is high chance of improperly made data [18], so unsupervised learning with k-means is employed to predict as in [20].In [21] a mechanism for handling delay sensitive and resource constraint client devices like cameras ,security alarms is considered thus investigating the QoS of IoTSHS but they ignore the effect of malicious nodes among the QoS traffic path.[22] shows that instead of maximizing the QoS, which is generally energy costly, better energy efficiency can be achieved by targeting satisfactory QoS levels only. The approach aims to enhance energy efficiency while ensuring a desired QoS threshold. In[23]highlightsthe QoS requirements of smart services andthe mechanisms employed by standards in enabling interoperability and QoS.As from the above study we can see how much QoS is important aspect in IoTSHS. Here we utilized dualcommunicationlink technologies as suggested by [19] to provide the optimized alternative path for QoS in case malicious node is detected.

III. Methodology

This section has components overview and followed by Proposed system to realize IoTSHS.

The following components are used to implement the IoTSHS

A. Raspberry Pi

B. Node MCU (ESP8266)

C. Humidity and temperature sensor (DHT11)

D. Bluetooth module (HC-05)

E. Relay board

F. Blynk Application in mobile phone

A. Raspberry Pi

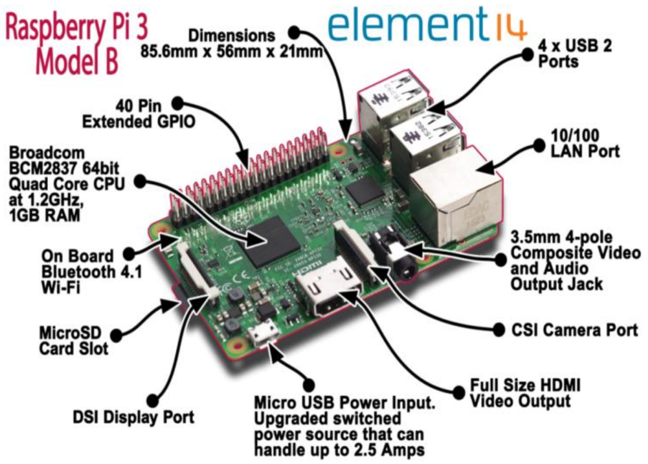


Figure 3.Raspberry Pi

Raspberry Pi isARM processor based SoC (System of Chip) by Broadcom.Asthe RAM and processing power are very low compared to today's mobile phones and laptops, because of this it is low cost computer good for IOT based projectsespecially for Proof of concept demonstrations. In our project wepreferred it as it can be easily programed to be gateway, with both Wi-Fi access point and IOT node capability.We could use packet capture and analysis in raspberry pi because of many software development tools available thus making our development cycle fast.

B. NodeMCU (ESP8266)

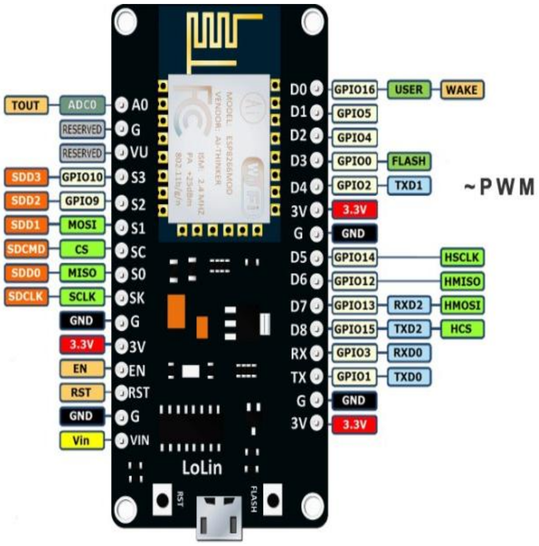


Figure 4.Node MCU

Node MCU is an IoT based platform which runs on the ESP8266 Wi-Fi SOC from Espressif Systems. Hardware is based on the ESP-12 module. The term "Node MCU" by default refers to the firmware rather than the dev kits. We have selected this as it has inbuilt Wi-Fi capability and large set of libraries for different IOT devices. In our project it acts as a wireless IOT clientnodes, capable of periodic sensor data collection and controlling the actuators. They assist in extending the Wi-Fi capability for entire home thus the number of Client node depends on each user's home layout.

C. Humidity and Temperature Sensor (DHT11)

Figure 5.DHT11 Sensor

Temperature and Humidity sensors detect the valuesas a percentage of the immediate environments in which they are placed. We are using this sensor because of its cost effectiveness and relative higher accuracy. In our system with this sensor we want to do a basic demonstration that how the sensor data be collected, how can we do in system error correction and avoid false data pushing to cloud infrastructure. The sensors are integrated serially with Node MCU via there GPIO pins.

D. Bluetooth Module (HC-05)

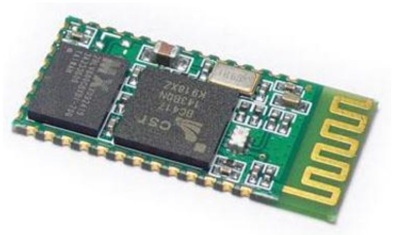


Figure 6.HC-05 BT module

HC-05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup. Serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR (Enhanced Data Rate) 3Mbps Modulation with complete 2.4GHz radio transceiver and baseband. We can configure each device as master or slave via the attention commands (AT). In our project they are used as a one more communication link for the alternative path. This communication link is used when detecting fault node and also when an alternative path is selected for QoS data. The same link can also be used in case of link failures. They are preferred because of easy integration capability available in Node MCU.

E. Relay Board

Figure 7.Relay Board

A relay is an electromagnetic switching device consisting of an armature which is moved by an electromagnet to operateone or more switch contacts. Some advantages of relays are that they provide amplification and isolation and are straight forward. Here we are using 5v 4-channel relay interface board, and each channel needs a 15-20mA driver current.it can be used to control various appliances and equipment with large current relays that work under AC250V 10A or DC30V 10A.it has a standard interface that can be controlled directly by microcontroller.

F. Blynk Application on Smartphones

Blynk is third party app which has interfaces in both iOS and Android phonesmainly used to control Node MCU, Raspberry Pi.The graphic interface can be built in the digital dashboard by simply dragging and dropping widgets.It is provided asa tool for user to makeIOT design automation.

Proposed System:

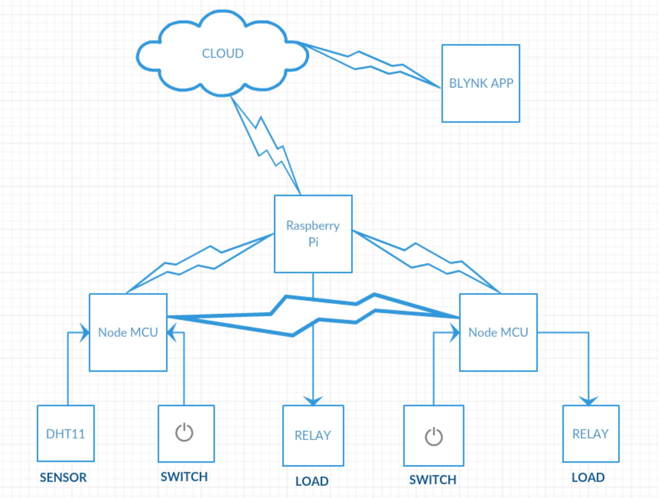


Figure 9.Proposed System block diagram

The proposed system is as shown in figure 9 which is implemented using Node MCU,due to its cost effectiveness and ease of development. In this method, all the sensors are connected to the Node MCU board and the results can be seen in Smart phone via a Blynk app. In our simulation setupTemperature variation is detected by the sensor. This will trigger the system to turn on the relay which intern controls the fan to regulate the temperature. We will collect all required statistics from nodes. AI technique is used to analyze all these captured statistics to derive at user pattern. Example being traffic bandwidth requirement of each node based on traffic from connected sensor.

K-means clustering is a method used for determining the malicious node.The “K” refers to the number of clusters specified.Gateway node checks the received packets integrity from each path andthen computes a contribution metric (trustworthiness level) of each node along a path. The contribution metric is then used as feature to identify the node’s behavior. The Gateway nodes make the feature calculations (trustworthiness of nodes) more accurate and the malicious node identification process effective. Nodes are clustered into malicious or benign groups based on their contribution levels extracted at the Gateway nodes

Overview of Algorithm:

1. The sample space is initially partitioned into K clusters and the observations are randomly assigned to the clusters.

2. For each sample:

- Calculate the trustworthinessof nodes falling in the sample path.

- IF the sample is closest to its own cluster THEN leave it ELSE select another cluster.

3. Repeat steps 1 and 2 until no observations are moved from one cluster to another.

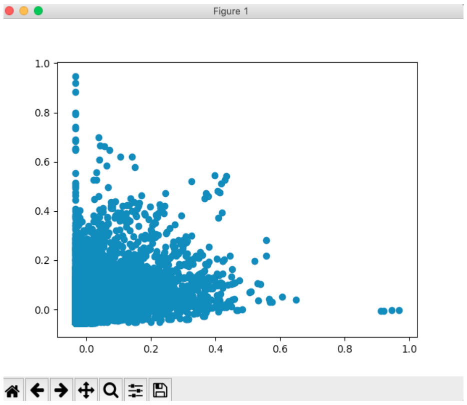


Figure 8.K-means algo output

As shown in figure 1, Sensors and actuators are connected to nodes via the GPIO's.Raspberry Pi and Node MCU modules are connected using 2.4 GHz Wi-Fi backhauland Bluetooth Point to Point link as a dual communication link shown in figure 2. Here Raspberry pi is acting as Gateway node. The sensor data is collected by the Node MCU models which are acting as an IOT Nodes connected to internet via the gateway node.Various statistics of nodes like bandwidth requirement, channel utilization, physical data rate, traffic patterns are stored and processed in cloud. Sensor data with statics is periodically updated in Blynk application as shown in above block diagram figure 9.

A node under attack will manipulate each packet it forwards by a fixed probability. Thus K-means can be used in cloud to detect a malicious node via dual link technology [20]. Each node gets the malicious node info and on detecting the malicious node in the next hop path, alternative path is activated thusavoiding the path to malicious node. In our case, as an alternative path cloud software will instruct the Bluetooth module connected within each node to get activated and transfer data towards cloud.The flow chart on IOT nodes is shown in figure 10.

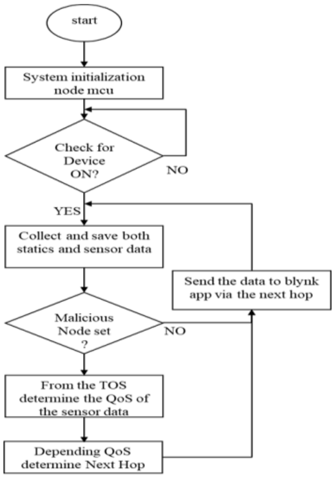

start
System initialization node mcu
Check for Device ON?
NO
YES
Collect and save both statics and sensor data
Send the data to blynk app via the next hop
Malicious Node set ?
NO
From the TOS determine the QoS of the sensor data
Depending QoS determine Next Hop

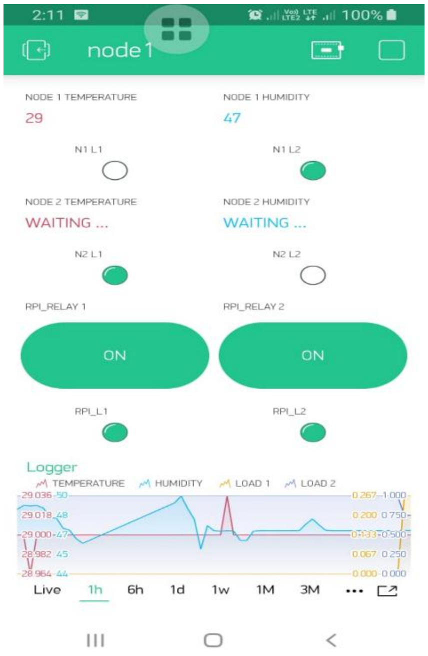
Figure 10.Flow chart for Nodes

IV. Results and Discussion

The result that have been obtained from above setup can be seen in Blynk app as captured below.As shown in figure 11 Blynk app is programmed to display Node 1 and node 2 data with temperature sensor values. Switch status from the Gateway node is indicated via the marking L1 to L4 where the red indicates the ON status of the relay Load. There is logger window to show the data collected over a time period.

By collecting statistics from all nodes, the cloud applies votingtoidentifywhetheranodeismaliciousornot. We use the packet manipulation attack model. The compromised nodes can report falsified information about their neighbors, i.e., report malicious nodes as normal and normal nodes as malicious, which is what we assumed here. It is observed from Fig. 12 that, when the malicious nodes areinducing the falsified temperature data then it takes some time to regulate the data depending on different alternative paths, the temperature value eventually normalizes.

The computational burden in our approachesismovedfromthesimplenodes to the more powerful Cloud infrastructure


NODE 1 TEMPERATURE 29

NODE 1 HUMIDITY 47

N1 L1 ○

N1 L2 ●

NODE 2 TEMPERATURE WAITING ...

NODE 2 HUMIDITY WAITING ...

N2 L1 ●

N2 L2 ○

RPI_RELAY 1 ON

RPI_RELAY 2 ON

RPI_L1 ●

RPI_L2 ●

Figure 11.Normal scenario result as captured in Blynk App.

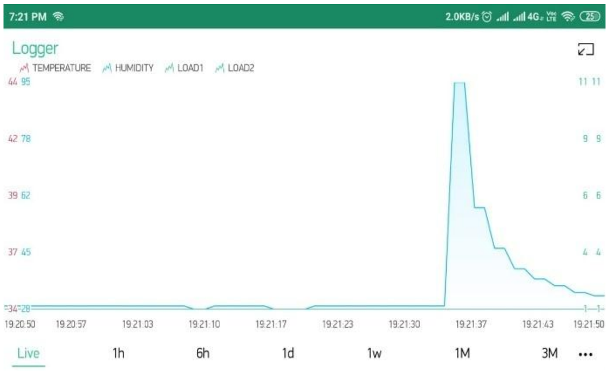


Figure 12.malicious node simulation by inducing the fixed error

V. Conclusion and Future Scope

IoTSHS can be implemented using the cost effective IOT components.By using Dual link technology with k-means algorithm we can detect a malicious or faulty node. Using this information alternative path for QoS data is chosen.Thus, we have demonstrated that the proposed system can be effectively used for collecting client device statistics.From our methodology we have shown to integrate Sophisticated AI technique to IoTSHS to analyse each home user.With the observation made from our system we have concluded that Malicious Node detection mechanisms itself will not be sufficient for IoTSHS. For best user experience and better security management, Providing the alternative route to QoS data is also necessary for optimal functionof IoTSHS.

For future we should Considering more client statistics like Interference, House layout,Type of Application, Number of connected devices, Frequency channels.And Provide a more fast, accurate results in fault node detection and selecting alternative path for QoS data.

REFERENCES

[1] C. Withanage, R. Ashok, C. Yuen, and K. Otto, "A comparison of the popular home automation technologies," in Innovative Smart Grid Technologies-Asia (ISGT Asia). IEEE, 2014, pp. 600–605.

[2] J. Zheng and M. J. Lee, "A comprehensive performance study of ieee 802.15. 4," Sensor network operations, vol. 4, pp. 218–237, 2006.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.

[4] S. Kriaa, M. Bouissou, and L. Pi`etre-Cambac´ed`es, "Modeling the stuxnet attack with bdmp: Towards moreformalriskassessments,"in7thInternational Conference on Risk and Security of Internet and Systems (CRiSIS). IEEE, 2012, pp. 1–8.

[5] S.J.Shackelford,A.A.Proia,B.Martell,andA.N. Craig, "Toward a global cybersecurity standard of care: Exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices," Tex. Int'l LJ, vol. 50, p. 305, 2015.

[6] C.Wang,T.Feng,J.Kim,G.Wang,andW.Zhang, "Catching packet droppers and modifiers in wireless sensor networks," IEEE Transactions on ParallelandDistributedSystems,vol.23,no.5,pp. 835–843, 2012.

[7] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. of the 13th European Wireless Conference, 2007, pp. 1–10.

[8] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyberphysical networked systems," IEEE Transactions on Computers, vol. 64, no. 1, pp. 4–18, 2015.

[9] M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, "Distributed detection in mobile access wireless sensor networks under byzantine attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 4, pp. 950–959, 2014.

[10] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks," in IEEE International ConferenceonCommunications. IEEE,2009,pp. 1–6.

[11] M. Abdelhakim, L. Lightfoot, J. Ren, and T. Li, "Reliable communications overmultihop networks under routing attacks," in Global Communications Conference(GLOBECOM). IEEE,2015,pp.1–6.

[12] M. Abdelhakim, X. Liu, and P. Krishnamurthy, "Diversityfordetectingroutingattacksinmultihop networks," in International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018, pp. 1–6.

[13] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE, 2007, pp. 335–340.

[14] J. F. C. Joseph, B.-S. Lee, A. Das, and B.-C. Seet, "Cross-layer detection of sinking behavior in wireless ad hoc networks using svm and fda," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 233–245, 2011.

[15] A. I. Moustapha and R. R. Selmic, "Wireless sensor network modeling using modified recurrent neural networks: Application to fault detection," IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 5, pp. 981–988, 2008.

[16] D. Janakiram, V. Reddy, and A. P. Kumar, "Outlier detection in wireless sensor networks using bayesian belief networks," in First International Conference on Communication System Software and Middleware. IEEE, 2006, pp. 1–6.

[17] K. Leung and C. Leckie, "Unsupervised anomaly detection in network intrusion detection using clusters," in Proceedings of the Twenty-eighth Australasian conference on Computer Science, vol. 38. Australian Computer Society, Inc., 2005, pp. 333–342.

[18] S. Ruoti, S. Heidbrink, M. O'Neill, E. Gustafson, and Y. R. Choe, "Intrusion detection with unsupervised heterogeneous ensembles using cluster-based normalization," in IEEE InternationalConferenceonWebServices. IEEE, 2017, pp. 862–865.

[19] Xin Liu, Mai Abdelhakim, Prashant Krishnamurthy, David Tipper, "Identifying Malicious Nodes in Multihop IoT Networks using Dual Link Technologies and Unsupervised Learning" Open Journal of Internet of Things (OJIOT) Volume 4, Issue 1, 2018

[20] Tiankai Liang , Bi Zeng, Jianqi Liu, Linfeng Ye,Caifeng Zou "An Unsupervised User Behavior Prediction Algorithm Based on Machine Learning and Neural Network For Smart Home" IEEE Access (Volume: 6),Page(s): 49237 – 49247,Page(s): 812 – 821

[21] Irfan Awan, Muhammad Younas, Wajia Naveed "Modelling QoS in IoT Applications" 2014 17th International Conference on Network-Based Information Systems

[22] Hajar Elhammouti, Essaid Sabir, Mustapha Benjillali, Loubna Echabbi, Hamidou Tembine, "Self-Organized Connected Objects: Rethinking QoS Provisioning for IoT Services" : IEEE Communications Magazine (Volume: 55 , Issue: 9 , Sept. 2017)Page(s): 41 – 47

[23] Oladayo Bello, Sherali Zeadally,"Toward efficient smartification of the Internet of Things (IoT) services"Future Generation Computer SystemsVolume 92, March 2019, Pages 663-673

Authors Profile

Dr.Arun Biradar is woring as a professor and Head in Department of computer science Engg., East West Institute of Technology. He has published more than 50 research papers in national and international coferences and journals. His research areas are Wireless Ad-Hoc networks, Computer Networks, Software Engg., Genetic Algorithms and Machine Learning.

Mr.B R Susheel kumar pursed Bachelor of Engg. from VTU University in year 2005. and currently pursuing M.tech in Department of Computer Network Engineering, VTU since 2017.