International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 103-116
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Mamdani Fuzzy Logic System based Merkle Technique (M-FLS-MT) for Malicious Node Detection in Wired and Wireless Networks

[1]R. Karthik, [2]S. Veni and [3]B.L. Shivakumar

[1]Department of Information Technology,

Kongunadu Arts and Science College,

Coimbatore.

[2]Department of Computer Science,

Karpagam Academy of Higher Education,

Coimbatore, India.

[3]Sri Ramakrishna Polytechnic College,

Coimbatore, India.

Abstract

Network security is an ever demanding thrust research area in the field of computer science and research. Providing reliable and secured network is a stupendous task. As far as network security is concerned, applying soft computing techniques fact such as fuzzy logic is emerging its peak. This research work aims to design and develop theMamdani Fuzzy Logic System based Merkle Technique (M-FLS-MT) for Malicious Node Detection. KDD cup'99 dataset contains four main types of attacks in the system is selected for performing M-FLS-MT classification. Performance metrics detection rate and false alarm rate are selected.

Key Words: Classification, data mining, networks, detection rate, false alarm rate.

1. Introduction

Security issues are intensified because of briefing way and in addition, lasting self-assertive disappointments are ordinary in networks, and these disappointments might be utilized by foes as powerlessness. The significant excess in networks prompts magnificent potential in outlining them for proceeding with their arrangement of particular administration in spite of disappointments. For meeting practical framework necessities which is seemingly perpetual and the unattended operations, and remote sensor networks should be fit for proceeding with capacities in an attractive way within the sight of, and, recoup viably from security strikes. The framework should be equipped for adjusting to novel, unforeseen ambushes when the framework is at first sent. Trust foundation among nodes is an imperative for assessing trustworthiness of different nodes since survival of remote sensor networks is dependent on community oriented and in addition trusting nature of the nodes. Security and in trust aretwo great degree between subordinate ideas and between reliance terms are utilized as equivalent words, when characterizing secure frameworks. When, security cannotbe taken as trust, the essential distinction is more entangled and has higher overheads. Trust in networks has a noteworthy part to play in building networks and including or erasing nodes from networks, in the development of the network, or supplanting falling flat or undependable nodes in a smooth and also straightforward way. Making, working and also overseeing networks are dependent on the agreeable and trustworthy nature of nodes; subsequently, trust foundation between nodes is an imperative.

2. Literature Review

In [1] the author hasproposed a plan for the circulated detection of versatile malignant hub assaults. Their plan applies the Sequential Probability Ratio Test (SPRT) to distinguish hubs that have left a locale which cannot send messages to their neighbours. The creators demonstrated that their plan identifies any versatile vindictive hub rapidly, and that a portable noxious hub can just stay away from detection for an extremely constrained era. Their re-enactment comes about demonstrated that their plan rapidly distinguishes portable malevolent hubs with only a couple of tests and with small false positive and false negative rates.

In the literature [2], trust systems for specially appointed lattice processing conditions are broken down. The creator has proposed a trust based plan called as RETENTION: a receptive put stock in based component to recognize and rebuff noxious hubs in specially appointed network conditions. The primary goal of their plan is to perform accurate disciplines of vindictive hubs utilizing the best-broke down put stock in show. As indicated by their outcomes, the creators asserted that RETENTION is an effective component to identify and rebuff vindictive hubs in specially appointed matrix situations.

The authors of the literature [3] has proposed Trust-based Exclusion Access-Control Mechanism (TEAM) in order to guarantee that lone helpful hubs can get to the system by barring the acting mischievously. Group separates the entrance control obligation into two settings; nearby and worldwide. The nearby setting obligation is the area watch to advise the worldwide setting about suspicious conduct. In its turn, the worldwide setting investigates the got data and chooses whether it rebuffs the suspicious hub utilizing a voting plan.

In the literature [4] the authors have modelled the malevolent hub detection process as a Bayesian amusement with blemished data and demonstrated that a blended strategy idealize Bayesian Nash Equilibrium is feasible. The creators additionally indicated how a malignant hub can develop a conviction about the conviction held by a general hub. By utilizing the conviction about the conviction framework, a Markov Perfect Bayes– Nash Equilibrium is introduced and the balance delays the detection of the noxious hub.

The authors of [5] has proposed a model that distinguishes the assault before it occurs with early cautioning notices to reveal interlopers while arranging the phases of an assault. Observing past warning when oddity blockage surfaces is valuable for sifting noxious movement and limiting potential overhead and assets related with interruptions.

In [6] the authors have proposed a scheme which is to ensure that does not exclusively do the base station hub and does not acknowledge the manufactured total outcomes, but rather likewise the vindictive aggregators messing with the middle outcomes can be distinguished. The ill-disposed aggregators, after detection, can be removed from the system, consequently lessening the harm of vindictive aggregators.

The authors of the literature [7] introduced another improvement display in the guard of parcel based assaults. Their ideal assessment focuses the issue and finds a subset of handling units in the shrewd matrix that can fit for review through the position of the profound bundle controllers with the goal to amplify the quantity of investigated parcels and catch pernicious ones under the given limitations. The creators guaranteed that their different sweep situations are difficult to actualize the present system structure and moreover turn the calculation according to the plan.

In [8] the authors have discussed mainly on the most effective method to distinguish malignant associates utilizing theanomaly mining approach in mixture P2P networks. The creators have influenced utilization of nearby incessant conduct to design mining process and the worldwide continuous conduct design delivering approach by incrementally spreading and totalling the neighbourhood visit conduct designs. In light of the nearby continuous examples and the worldwide incessant examples, the creators have anticipated the vindictive hub detection process.

The authors of [9] haveproposed Categorization of Malicious Behaviours utilizing Cognitive Agent (CMBCA) which is a wise multi operator framework used to identify known and obscure noxious exercises completed by clients over a system. CMBCA is completely self-sufficient and once instated screens entire networks with the assistance of psychological versatile specialists.

3. Proposed

Background of Merkle Tree Scheme

This research paper applies the merkle tree principle [14] for performing information security. Ralph Merkle has developed the idea of merkle tree or hash tree to make safe confirmation of the reports amid the transmission. In this tree, the non-leaf hub comprise of the hash of the qualities is shown in the leaf hub. This plan utilizes one open key to sign several reports, and the conceivable amount of reports is $N = 2^N$. The Fig.1 proves an example of merkle tree which generate, public keys X_i and private keys $Y_i$of 2n. The hash value is calculated as follows:

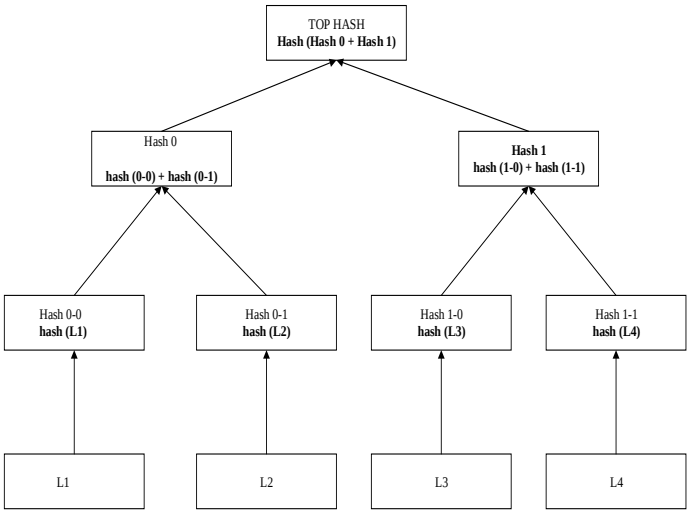

Figure 1: Merkle Tree

For each private key $Y_{i,}$ 1<= i<=2n

$$h_i = H(Y_i) \quad (1)$$

The hub in the merkle tree is signified by a_{ij} where *i*means the level of a hub, *j*means the numeral of the hub and $h_i$means the leaf hub of the merkle tree. The internalhub of the hash tree is the concatenated hash value of its kidhubs. From the Figure 2, the hash value is:

$$a_{1,0} = H(a_{0,0} \,||\, a_{0,1}) \quad (2)$$

$$a_{2,0} = H(a_{1,0} \,||\, a_{1,1}) \quad (3)$$

The root estimation of the tree $\boldsymbol{a}_{n,0}$ is the public key **(pub)** generated and this

value is confirmedat a point in the conduction and if there is any alter in the **pub**, then there willsubsist some malevolentbustle. This investigate work applies merkle tree for message confirmation in the ad hoc routing environment.

Fuzzy Model

This paper proposes a fuzzy based approach to identify the malicious hub in the network. Fuzzy rationale is the multi-esteemed rationale acquired from the fuzzy set hypothesis and the likelihood esteem series from 0 to 1 [13]. The fuzzy set [10] hypothesis is connected to assess the honesty of the center in the system. The Fig.2 gives the general engineering of FLS. The fresh contributions from the information factors is connected to the fuzzy motor to make the fuzzy sets, and this procedure is called as fuzzification [15].

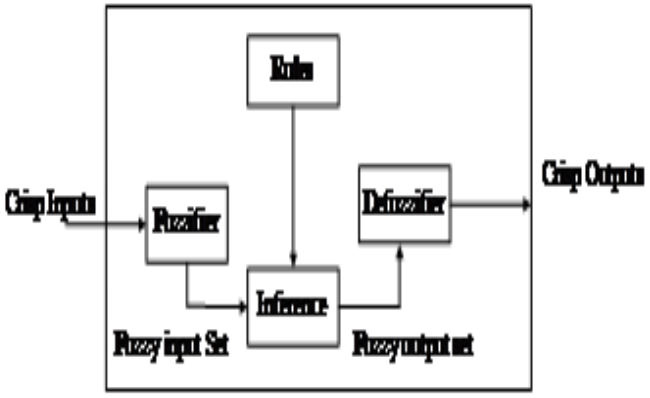

Figure 2: Fuzzy Logic System

The fuzzified esteems are given as the contribution for the suggestions or guidelines like IF-THEN to take care of the control issues [12] which deliver a fuzzified yield esteem. This esteem shows the put stock in estimation of the sensor center and is connected to the defuzzification module to get the non-fuzzy yield. The future fuzzy trust demonstrates produces the evaluated trust esteem and its connection with the trust limit decides the reliability of a center point.

Merkle approach [14] applies centralized security evaluation scheme, in which the top hub or root hub of the hash tree plays a major role. During the transmission between two entities, the root value or hash value is verified, if it is altered, then the transmission is identified as malicious. In this method, identifying the malicious hubs is difficult because the intruders may exist as an intermediate hub or the source. The existing scheme [11] doesnot provide suitable differentiation scheme to identify the malicious hub. Also, the root value can easily altered by the intruders, which makes this method less secure. So, this shortcomings of existing scheme motivates to develop strong IDS with less resource consumption. The proposed method applies fuzzy logic to identify the malevolenthubs with minimal sourceutilization.

Prototype of the Proposed Method

The vitality esteem and trust esteem are the etymological factors to the fuzzy framework as depicted in the Fig.3. These factors are decayed to the phonetic terms.

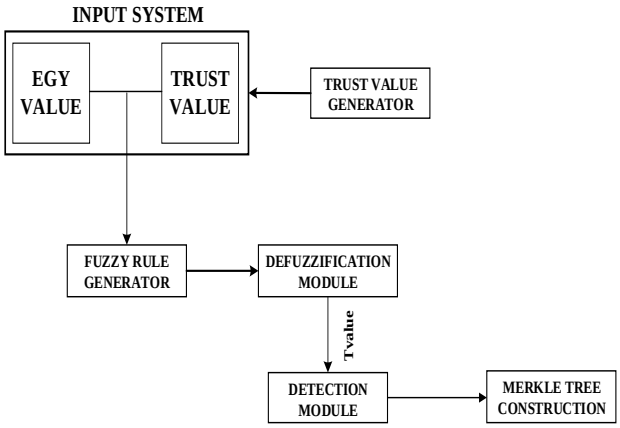

Figure 3: IDS Architecture

1. Energy Variable

Let the energy (egy) is the linguistic variable which speaks to the energy estimation of the center points in the system. To succeed the linguistic estimations of the energy, and words, "low" and "high" values are utilized. These are the linguistic esteems to the energy. At that point, the accompanying condition gives the set of decomposition (E) for the linguistic variable energy.

$$E(e) = \{\text{very-low, low, medium, high, very-high}\} \quad (4)$$

2. Trust variable

Let the trust (spd) is the linguistic variable which speaks to the put stock in an incentive from the physical layer of the system. To qualify the linguistic estimations of the trust, and terms, example, "low" and "high" are values utilized. These are the linguistic esteems to the trust. At that point, the accompanying condition gives the set of decomposition (T) for the linguistic variable trust.

$$T(t) = \{\text{very-low, low, medium, high, very-high}\} \quad (5)$$

Algorithm 1 Energy Input ( )

{

Give egy a chance to be the information energy to the fuzzy framework, EGY_HI be the ideal estimation of energy, EGY_LOW be the lower estimation of energy If (egy > EGY_HI) Return HIGH;
Else if (egy< EGY_LOW) Return LOW;

Else Return MEDIUM;

}

Algorithm -1 Description

The energy is given as the contribution to the fuzzy framework and if, the esteem is higher than the given ideal esteem, the fuzzy framework reacts with the energy a high esteem. In that event, the energy esteem is not as much as the given ideal esteem, the fuzzy framework reacts with the energy of low esteem or else the energy medium value.

Algorithm 2 Trust Input ( )

{

Give spd a chance to be the information trust an incentive to the fuzzy framework which is gotten from the physical layer, TRUST_HI be the ideal estimation of trust, TRUST_LOW be the lower estimation of trust

If (spd > TRUST_HI) Return HIGH;

Else If (spd < TRUST_LOW)

Return LOW;

Else Return MEDIUM;

}

Algorithm -2 Description

The trust is given as the contribution to the fuzzy framework from the remote physical layer and if, the esteem is higher than the given ideal esteem, the fuzzy framework reacts with trust high esteem. On the off chance that, the trust esteem is not as much as the given ideal esteem, the fuzzy framework reacts with trust low esteem or else the trust medium esteem.

Algorithm 3 Fuzzy rule ( )

Fuzzification process obtains the fuzzy set using fuzzy linguistic variables, fuzzy linguistic terms and membership functions. Table 1 list the fuzzy rules applied.

Table 1: Fuzzy Rules

n_1(egy)	n_2 (spd)	Result
Low	Low	Very Low
Low	Medium	Low
Low	High	High
Medium	Low	Very low
Medium	Medium	Low
Medium	High	Medium
High	Low	Very low
High	Medium	High
High	High	Very high

Algorithm – 3 Descriptions

Let n_1, andn_2 denote the input linguistic factors given to the fuzzy induction motor, where $n_1$implies the energy and n_2 implies the trust from the physical layer. The fuzzy control is connected to recognize the center confide in an incentive with the use of fuzzified energy and put stock in values.

Algorithm 4 Defuzzification ( )

{

If (rule=LOW) Return (0, LOW)

If (rule=MEDIUM) Return (LOW, MEDIUM)

If (rule=HIGH) Return (MEDIUM, HI)

If (rule=VERYHIGH)

Return (HI, VERYHIGH)

Return (0, 1)

}

Algorithm -4 Description

Defuzzification is the way toward exchanging the totaled fuzzy yield to a fresh yield esteem [10]. The defuzzification module exchanges the fuzzified trust an incentive to ordinary confide in esteem. On the off chance that the fuzzy control creates LOW as yield, at that point the IDS haphazardly produces the trust esteem and it is returned. So also, the IDS return irregular esteems for MEDIUM, HIGH, and VERY HIGH et cetera. The last put stock in esteem (Tvalue) is returned in the interim of [0, 1].

Algorithm 5 Detection ( )

{

Get Tvalue from the defuzzification module,

Let Trust_Threshold = 0.4;

If (Tvalue <= Trust_Threshold)

{

Add the Hub ID to the malicious list and broadcast the Hub ID. Remove the Malicious hub from the tree….

Start new Merkle tree formation.

}

}

Algorithm -5 Description

The trust estimation of the part centers is extricated from the defuzzification module. The trust edge is set as 0.4. On the off chance that, the trust estimation

of the center points are not as much as the put stock in edge, at that point the center point might be a pernicious center and added to the rundown to be specific noxious rundown. The center point ID of the malignant center is communicated to the neighboring center points and expels the malevolent center from encourage bundle sending process.

4. Results and Discussions

The KDD Cup 1999 dataset utilized as in [16], [17] is utilized for benchmarking interruption location issues in the exploration work. The dataset are a gathering of recreated crude TCP dump information over a phase of nine weeks on a neighbourhood. The preparation information is handled in concerning five million associations records from seven weeks of system activity and two weeks of testing information built up around two million association records. The direction information is comprised of 22 distinct assaults out of the 39 in the test information. The perceived assault sorts are those current in the direction dataset while the novel assaults are the extra assaults in the test datasets not existing in the preparation informational indexes. The assaults sorts are gathered into four classifications:

DOS: Denial of service – e.g. syn flooding.

Probing: Surveillance and other probing, e.g. port scanning.

U2R: unauthorized access to local super user (root) privileges, e.g. buffer overflow attacks.

R2L: unauthorized access from a remote machine like password guessing

The training dataset consisted of 4,94,021 records among which 97,277 (19.69%) are normal, 3,91,458 (79.24%) DOS, 4,107 (0.83%) Probe, 1,126 (0.23%) R2L and 52 (0.01%) U2R connections. In every connection, 41 attributes describe the different features of the relationship and a tag is assigned to every either as an attack type or as normal. Imitation outcome shows that the projected M-FLS-MT attains better detection rate and reduced false alarm rate [18].

Table 2: Detection Rate

Algorithms	**DoS**	**Probe**	**U2R**	**R2L**
M-FLS-MT	99.1	99.4	98.9	78
PSO with SVM [16]	97.9	98.6	68.9	19.5

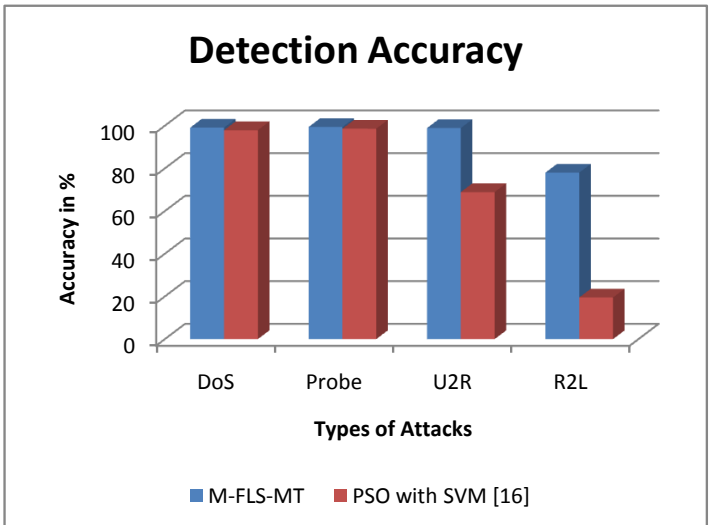

Figure 4. Detection Rate

Table 3: False Alarm Rate

Algorithms	DoS	Probe	U2R	R2L
M-FLS-MT	0.9	0.6	1.1	22
PSO with SVM [16]	2.1	1.4	31.1	80.5

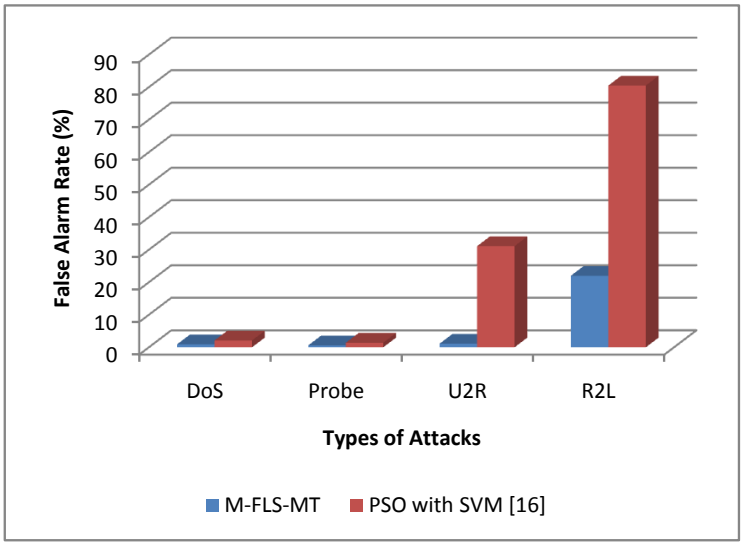

Figure 5: False Alarm Rate

5. Conclusions

This paper presents Mamdani Fuzzy Logic System based on Merkle Technique (M-FLS-MT) for Malicious Hub Detection. KDD cup'99 dataset contains four

main types of attacks in the system is selected for performing M-FLS-MT classification. Performance metrics detection rate and false alarm rate are selected. Simulations are conducted using MATLAB tool. From the results it is evident that M-FLS-MT obtains better detection rate for all types of attacks and also the false alarm rate is reduced considerably.

References

[1] Jun-Won Ho, Matthew Wright, Sajal K.D., Distributed detection of mobile malicious node attacks in wireless sensor networks, Ad Hoc Networks 10 (3) (2012), 512-523.

[2] Braga R.B., Chaves I.A., De Oliveira C.T., Andrade R.M., De Souza J.N., Martin H., Schulze B., RETENTION: A reactive trust-based mechanism to detect and punish malicious nodes in ad hoc grid environments, Journal of Network and Computer Applications 36 (1) (2013), 274-283.

[3] Ferraz L.H.G., Velloso P.B., Duarte O.C.M., An accurate and precise malicious node exclusion mechanism for ad hoc networks, Ad hoc networks 19 (2014), 142-155.

[4] Wenjing Wang, Mainak Chatterjee, Kevin Kwiat, Qing Li, A game theoretic approach to detect and co-exist with malicious nodes in wireless networks, Computer Networks 71 (2014), 63-83.

[5] Abdulghani Ali Ahmed, AmanJantan, Tat-Chee Wan, Filtration model for the detection of malicious traffic in large-scale networks, Computer Communications 82 (2016), 59-70.

[6] Hongjuan Li, Keqiu Li, Wenyu Qu, Ivan Stojmenovic, Secure and energy-efficient data aggregation with malicious aggregator identification in wireless sensor networks, Future Generation Computer Systems 37 (2014), 108-116.

[7] Subhankar Mishra, Thang N.D., My T.T., JungtaekSeo, Incheol Shin, Optimal packet scan against malicious attacks in smart grids, Theoretical Computer Science 609 (2016), 606-619.

[8] XianfuMeng, Shuang Ren, An outlier mining-based malicious node detection model for hybrid P2P networks, Computer Networks 108 (2016), 29-39.

[9] Umar Manzoor, SamiaNefti, YacineRezgui, Categorization of malicious behaviors using ontology-based cognitive agents, Data & Knowledge Engineering 85 (2013), 40-56.

[10] Zadeh L.A., Fuzzy Sets, Information and Control 8 (1965), 338-353.

[11] AbderrahmaneBaadache, Ali Belmehdi, Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks,

Journal of Network and Computer Applications 35 (2012), 1130-1139.

[12] Sundararajan R.K., Arumugam U., Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor networks, Journal of Sensors (2015).

[13] Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li, Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications 35 (2012), 867-880.

[14] Jatinder Singh, Lakhwinder Kaur, Savita Gupta, A Cross-Layer Based Intrusion Detection Technique for Wireless Networks, The International Arab Journal of Information Technology 9 (3) (2012), 201-207.

[15] Kerim Goztepe, Designing a Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science 1 (1) (2012), 13-19.

[16] Sujitha B., Kavitha V., Layered Approach For Intrusion Detection Using Multi objective Particle Swarm Optimization, International Journal of Applied Engineering Research 10 (12) (2015), 31999 – 32014.

[17] Creech G., Hu J., A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontinuous System Call Patterns, IEEE Transactions on Computers 63 (4) (2014), 807 – 819.

[18] Karthik R., Veni S., Shivakumar B.L., Improved Extreme Learning Machine (IELM) Classifier for Intrusion Detection System, International Journal of Engineering Trends and Technology (IJETT) 41 (2) (2016), 66-71.

[19] RAJESH, M. "A SYSTEMATIC REVIEW OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATION." The Online Journal of Distance Education and e- Learning 5.4 (2017): 1.

[20] Rajesh, M., and J. M. Gnanasekar. "Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation." Computer Engineering and Intelligent Systems 6.8: 24-26.

[21] Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous WANET using FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974 (2015): 2115.

[22] Rajesh, M., and J. M. Gnanasekar. "Hop-by-hop Channel-Alert Routing to Congestion Control in Wireless Sensor Networks." Control Theory and Informatics 5.4 (2015): 1-11.

[23] Rajesh, M., and J. M. Gnanasekar. "Multiple-Client Information Administration via Forceful Database Prototype Design (FDPD)." IJRESTS 1.1 (2015): 1-6.

[24] Rajesh, M. "Control Plan transmit to Congestion Control for AdHoc Networks." Universal Journal of Management & Information Technology (UJMIT) 1 (2016): 8-11.

[25] Rajesh, M., and J. M. Gnanasekar. "Consistently neighbor detection for MANET." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.