IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012171 |

# An Efficient and Secured Trust Based IDS (Intrusion Detection System)

**Yenti Lakshmi Teja Sree**

Department of ECE, University College of Engineering Kakinada [A], JNTUK Kakinada, Andhra Pradesh, India

**ABSTRACT:** We can provide high-security in the current technological growth and is increasing day by day. To meet this requirement support vector machine cannotprovide high security. So,IDS(intrusion detection system)is used.Where IDS with key trust metrics layer and Fuzzy logic provides high security even there is an intruder. In this paper, key trust metrics layer has been presented. By using this we can provide high security and decrease energy and Overhead.

**KEYWORDS:** Support vector machine, Fuzzy logic,Key trust metrics layer.

## I. INTRODUCTION

In this day and age, utilization of wireless devices has expanded fundamentally with the advances in remote innovation. cognitive radio (CR) is a type of remote correspondence where a handset can keenly recognize which correspondence directs are being used and which are not. It immediately moves into empty channels while keeping away from involved ones. cognitive Radio is an idea acquainted with assault the forthcoming range.cognitive Radio users are unlicensed users who find unused authorized range powerfully for its own utilization without making any obstruction authorized users.Some of the current procedures utilized in Cognitive Radio incorporate range detecting, range data set and pilot channel. These methods are either perplexing that requires high computational ability to distinguish unused range or neglect to exploit range space made in genuine time.Cognitive radio (CR) is a promising innovation that comes to address the deficiency of the radio reach by giving utilization of the underutilized approved channels to accomplish higher reach efficiencyAncognitive radio (CR) has the limit (intellectual capacity) to recognize and aggregate information (like the transmission repeat, move speed, power, guideline, etc) from the overall climate. To build security we created Adaptive Multi-token based recognition component to defend the organization against flooding assault and dark opening assaults. In this a trust-based interruption identification framework is proposed to get the WSN by recognizing the aggressors at various layers.

The trust worth of a sensor node is determined utilizing the deviation of trust measurements at each layer as for the assaults. Primarily, we consider reliability in the three layers, for example, actual layer trust, media access control (MAC) layer trust, and organization layer trust utilizing FUZZY rationale and machine learning (SVM). The trust of a sensor node at a specific layer is determined by taking key trust measurements of that layer.

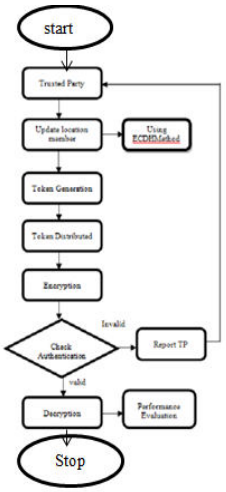



Fig.1.Adaptive multi token Flow chart

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012171 |

## II. ADAPTIVE MULTI TOKENAPPROCH

Location monitoring: The target of this progression is to give security that every sensornode recognizes a sufficient Number of objects to process an organization region .

Token management : The communication can be characterized into two distinct stages. They are, the key dissemination stage and the standard transmission stage. The organization condition and geographic messages are sent intermittently by nodes in the nonstop stage as they get enters progressively in the key appropriation stage. A gathering comprises of one gathering public key and many gathering private keys.

Elliptic Curve Diffie-Hellman (ECDH) Protocol: A shared key is created by ECDH protocol between two parties. Some public information is exchanged between two parties. Using this public data and private data these parties determines the shared secret key. Moreover, some third party, cannot access to the private details of all devices, and will not be able to analyze the shared secret from the accessible public information

## III. KEY TRUST METRICS LAYER

We can characterize assaults on cognitive radio organizations guarantees two things:

1. In decent protection to the licensedPU(primaryuser)
2. Missed opportunities for SU(secondary user)If the assault includes negligible tasks by the insignificant number of malevolent clients however making greatest misfortune or harm the essential or auxiliary clients in the organization

A few assaults are to explicit layer some cross layer assaults are multi-layer assaults that impact other layer.

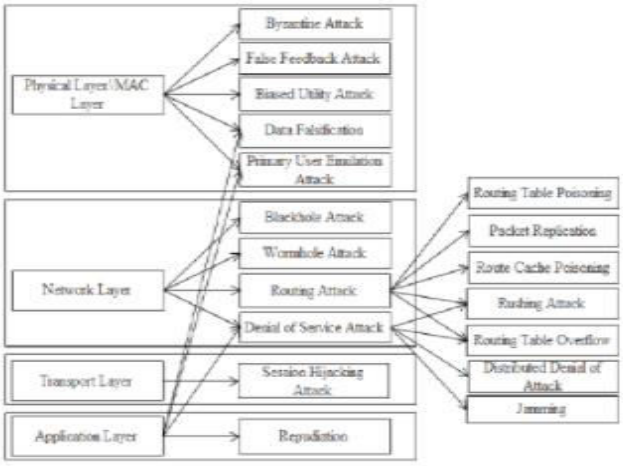



Fig:Cognitive radio Security network

## IV. SVM WITH FUZZY LOGIC

The SVM is a machine learning technique based on statistical methods. The SVM can be used for classification or regression analysis and its aim is to find the most optimal hyperplane.

Fuzzifier −The job of fuzzifier is to change over the fresh information esteems into fuzzy qualities.

Knowledge Base − It stores the information pretty much every one of the information yield fuzzy connections. It likewise has the participation work which characterizes the information factors to the fuzzy rule base and the result factors to the plant taken care of.

Fuzzy Rule Base − It stores the information about the activity of the course of space.

**Deduction Engine** − It goes about as a piece of any FLC. Fundamentally it recreates human choices by performing inexact thinking.

Defuzzifier− The job of defuzzifier is to change over the fluffy qualities into fresh qualities getting from fuzzy deduction engine

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012171 |

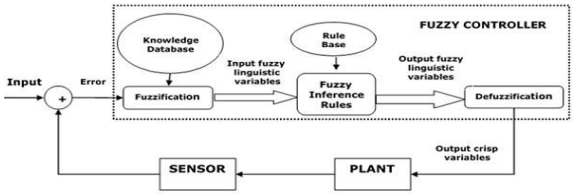
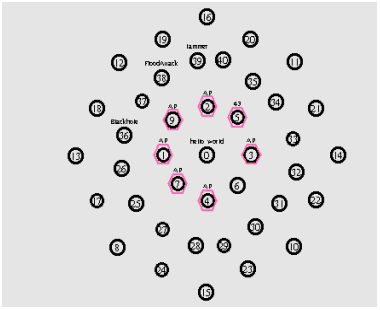
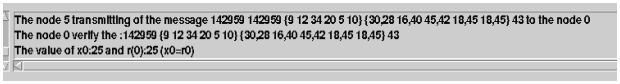



Fig :Architecture of Fuzzy Logic Control

This works fundamentally on to give security to cognitiveradio .The trust worth of a sensor node is determined utilizing the deviation of trust measurements at each layer regarding the assaults. Essentially, we consider dependability in the three layers, for example, actual layer trust, media access control (MAC) layer trust, and organization layer trust utilizing FUZZY rationale and machine learning(SVM). The trust of a sensor node at a specific layer is determined by taking key trust measurements of that layer and Adaptive Multi-token based recognition component to defend the organization against flooding assault and dark opening assaults, Obtained reenactment results show that Elliptic Curve Diffie Hellman convention alongside DRP convention has predominant execution in further developing information conveyance effectiveness and staying away from impacts



In Cognitive radio,we need Access points to transfer information there will be some attackers like jammers,Blackhole attack and flooding attack ,We must transfer the information from source to destination even there are attackers we will consider every node and detect and compare every node with threshold value Value greater than threshold are as Signature valid nodesValue less than threshold are called Signature invalidnodes




By detecting each and every node we can decrease Overhead and increase security and decrease energy.

## V. RESULTS AND DISCUSSION

This result clearly shows for solving inter-flow/intra
flow contention problems as well as hidden/exposed terminal problems. The proposed approach provides lesser overhead, Average overhead and dropped packet for selfish node with better packet delivery ratio and Latency than the existing Trust theory

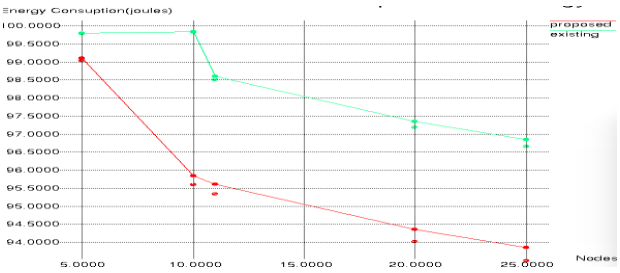



Fig-: Energy Consumption of proposed work with respect to proposed work

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012171 |

We used fuzzy logic with SVM so, energy consumption got decreased and provided more security

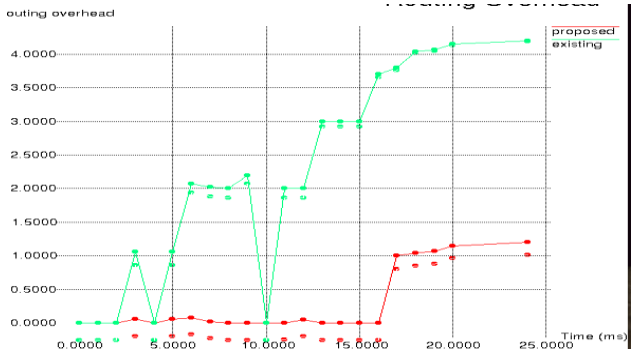



Fig- Routing Overhead of proposed work with respect to proposed work

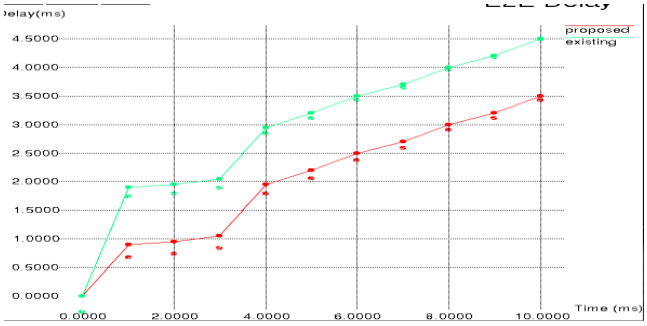



Fig: Delay comparison of proposed work with respect to existing work

TABLE I COMPARISON BETWEEN MODIFIED AND PROPOSED WORK

| Parameter | Modified work | Proposed work |
|---|---|---|
| Security | SVM provides less security | Key trust metrics layer provides more security |
| Delay | 45% | 33.02% |
| Overhead | 40% | 10.02% |

## VI. CONCLUSION

This project introduced Adaptive Multi-token based discovery instrument to shield the organization against flooding assault and dark opening assaults. This task has introduced the identification of limit exists for the comparable advocated new nodes and new absconded amounts. And furthermore proposed the security conserving, secure and ostensible Token-based rewarding. Which are utilized to disperse and gather the token. Acquired recreation results show that Elliptic Curve Diffie Hellman convention alongside DRP convention has predominant execution in further developing information conveyance proficiency and keeping away from crashes. This outcome plainly shows for settling between stream/intra-stream conflict issues just as covered up/uncovered terminal issues. And furthermore diminished postponement to 33% and just as overhead to 10% The proposed approach gives lesser overhead, delay.

## REFERENCES

[1]"Licensed and Unlicensed Spectrum Management for CognitiveM2M: A Context-Aware Learning Approach IEEE Transactionson Cognitive Communications and Networking" ( Volume: 6, Issue: 3, Sept. 2020), NianLiu,et al[1]
[2]"Secure Delegation-Based Authentication Protocol for Wireless Roaming Service:IEEE

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012171 |

CommunicationsLetters ( Volume: 16, Issue: 7, July 2012),Jia-Lun Tsai
[3]"An Efficient Key Predistribution Scheme in Wireless Sensor Networks",Published in: 2007 4th International Symposium on Wireless Communication Systems,17-19 Oct. 2007 ,Hangyang Dai
[4]"An Efficient Deep Learning Model to Infer User Demographic Information From Ratings",published in IEEE Access ( Volume: 7),17 April 2019,Yongsheng Liu
[5]"biquitous computing systems require new approaches to security".Result of the successful
EU Horizon 2020 Cost Action project Cryptacus Contributions from top-class researchers in security and cryptography. GildasAvoine.
[6]"Jian, Li, Li. Yun, JianRen and Jie Wu, 2014. "Hop-by-Hop message authentication and source privacy in Wireless Sensor " IEEE Transactions On Parallel and Distributed Systems, 25(5): 1223-123
[7]A Gateway Approach for Providing Nonlrtop IP Broadcasting Service Infrastructure Teruyuki Hasegawa, Tom Hasegawa (KDDI R&D Laboratories, Japan),TaekyoungKwon
[8]A Security and Privacy AwareLocationBasedRewarding System" IEEE Transactions on Parallel And Distributed Systems, 25(2): 343-353. Muhammad Adnan Tariq, Boris Koldehofe and Kurt Rothermel, 2014.
[9]. "A Secure Energy Mechanism for WSN and Its Implementation in NS-2," Wireless Communication, 72(4): 984-990. Pathak, G.R., S.H. Patil and J.S. Tryambake, 2014
[10]"Reliable Energy Aware Multi-Token Based MAC Protocol for WSN" IEEE International Conference on Advanced Information Networking and Applications, 43(8): 144-151.
[11]"Efficient and Trust Based Black Hole Attack Detection and Prevention in WSN," International Journal of Computer Science and Business Informatics, 14(3): 222-245. Rajendiran, K., R. Sankararajan and R. Palaniappan, 2011.
[12]. "Secure and efficient broadcast authentication in Wireless Sensor Networks" IEEE Transactions On Computers, 59(8): 1120-1133. Yeh, H.L., T.H. Chen, PC. Liu, T.H. Kim and H.W. Wei, 2011.
[13]. "Reliable Energy Aware Multi-Token Based MAC Protocol for WSN" IEEE International Conference on Advanced Information Networking and Applications, 43(8): 144-151.
[14]. "A secure key predistribution scheme for WSN using elliptic curve cryptography," ETRI Journal, 78(33): 791-801. Renubala, S. and K.S. Dhanalakshmi, 2014. "Trust based Secure routing protocol using Fuzzy Logic in Wireless Senor networks,"IEEE International conference on Computational Intelligence and Computing

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details