International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Trust based Intrusion Detection System Architecture for WSN

Abhishek Jain, Vishal Jain, Khushboo Tripathi

Abstract*: Today there are extraordinary attacks on all kind of networks. Security for Payload is considered one of the biggest agenda for all kind of organizations. To deal with new species if attacks like threat, which are blended in nature, no security platform can take guarantee for their intrusion protection. Among all security platforms, intrusion detection system (IDS) are being used to do the inspection of all the packets or data being transferred between two nodes, A software application , that is responsible doing the monitoring of any kind of unwanted or to monitor the activity which is malicious in nature. This research acquaints about handling unknown attacks through Intrusion Detection System. For improving security in wireless communication, Intrusion Detection System (IDS) plays significant role, which includes information about network and security scheme. Hence, this research paper focused on development of appropriate system architecture for IDS system

Keywords: IDS, IDS System Architecture, Trust Framework, Security, WSN.

I. INTRODUCTION

WSN , in the new ERA of new blended attacks is now more prone to CIA compromised by the attacks like Ransomware.

Ransomware [1] are the new class of blended attacks and new species of malware, which mainly uses file encryption to launch the attacks and ask for ransom money. There are mainly two categories of ransomware given by following:

1. Ransomware based on Encryption: In this category of ransomware, attacker encrypt the files of the OS of the machine being hacked and it will only decrypt in case when attacker will provide the decryption key. For instance: WannaCry

2. Ransomware based on Sensitive data: In this category of ransomware, attacker get the access to the PII information from the machine and blackmail the victim for the same. The various stages of ransomware stages are given by following:

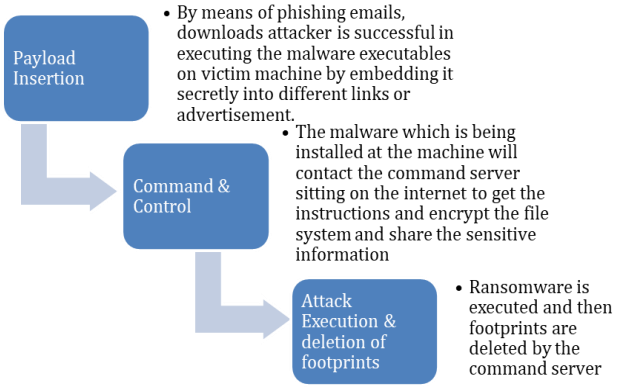

Fig. 1. Stages of Ransomware Attack

II. RELATED WORKS

Hwang R. J. and Huang Y. Z. (2016) [2] investigated about the WSN for securing data collected. This research focused on evaluation of smart card collected data from the sensor nodes. Sensor node provides confirmation about the transmit data and provides information to collector for provision of secure channel communication. By means of lightweight computation collector, evaluate the identity of card owner's. Evaluation results stated secure channel minimizes the cost of communication by means of data integrity, mutual authentication, and confidentiality, guessing of password, replay attack and malicious insider. Further, this approach reduces cost of communication. In future, the proposed approach is planned to integrate in Internet of Things.

Danyang Qin [3] suggested the routing approach for enhancing the Wireless Sensor Network security. Further, this technique efficiently reduces common control attack arise due to limited energy power and minimal deployment of transmission of data in WSN. The proposed scheme is referred as trust sensing based secure routing mechanism (TSSRM) with characteristics of lightweight and it has ability to resist against several attacks arise in common. In addition, this research perform security route selection approach through optimization with consideration of QoS metrics and trust. Results illustrated that TSSRM enhances the WSN security and efficiency. In other hand, TSSRM minimizes overhead of routing and recover data transmission reliability through mechanism of trust.

Divya Pandey, Vandana Kushwaha (2017) [4] reviewed about WSN and its applications. In addition, this research examines the WSN challenges, attacks, threats and challenges. In addition, this research evaluate the various parameters and attack in the WSN network with consideration of different categories.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Abhishek Jain*, department, Amity University, Gurgaon, India. Email: abhishekjain_25@yahoo.co.in
Vishal Jain department, BVICAM, New Delhi, India. Email: drvishaljain83@gmail.com
Khushboo Tripathi, department, Amity University, Gurgaon, India. Email: ktripathi@ggn.amity.edu.in

Attacks in WSN are classified with respect to different layer such as physical layer, data link layer and network layer. Through analysis, this research stated that attackers exhausted resources those are available in physical layer attack achieved by means of wireless channel radio signal transmission.

Sattar B. Sadkhan and Hussein Mohammed Salman (2017) [5] analyzed the wireless network architecture through disjoint-node multipath approach. This architecture involved in transmission and computation of architecture for operation. The developed algorithm does not requires any operation for arithmetic performance, which is based on linear system equation. Additionally, this research contract of suspect paths by means of (n-3) for reduction of number of operation for computation and transmission, which has been reduced with number of nodes.

Meenakshi Panda and Mohan Khilar (2015 [6] evaluated the challenges associated with Wireless sensor network. Security challenges are anticipated with respect to various layer of WSN stack protocol through identification of security threats. Detection and removal of threats in WSN is challenging where distribution of keys is complex job. Through analysis, it is stated that majority of security scheme involved in specified models of network and security model at all layers of WSN.

Suraj Sharma, Deepak Puthal,Sanjay Kumar Jena and Albert Zomaya, (2016) [7] developed a routing protocol based on cross-layer based multipath clustering. For analysis, nodes are deployed in random manner. To originate cluster formation of cluster this research utilizes control packet broadcasting with categorization of cluster head at various level. Simulation results demonstrated that proposed approach effectively improves the routing performance of WSN.

Y R. Chapman, T S Durrani, (2012),"[8] evaluated the network security through consideration of IP packet filtering. It focused on network security when packet are transmitted over the medium, which utilizes filtering of IP packet. Even IP packets are evaluated at application level gateway through IP contrast by means of alternative security network. Analysis stated that each packet is evaluated using filters and describes the securing protocol characteristics by means of packet filtering.

9. Vivek Katiyar, Prashant Kumar Narottam Chand (2011) [9] analyzed the application of WSN due to drastic evolution. The analysis demonstrated that WSN has been widely applied in disaster management, battlefield surveillance, and border traffic management etc. through deployment of sensor in the specified location. Even in this location, few nodes are unattended and attacked for WSN. Analysis of results stated that for reducing energy consumption clustering technique and increased lifetime has been utilized also this approaches improves the scalability of the network. Based on the energy efficiency classification of protocol are performed to improves network stability.

David Martins & Herve Guyennet., 2010 [10], talks about different category of attacks and their impacts. This gives us an idea about the recent and next generation attacks and their patterns.

Varsha Raghuwanshi and Umesh Lilhor, 2016 [11] researched on the DDOS category of attacks and its impact over WSN. Energy parameter is being used to do the mathematical calculation for the random value and Qualnet simulator is being used to carry out the experimental results.

S.G.Hymlin Rose & T.Jayasree, 2019 [12] worked on an important aspect for topology formation , particularly about the selection of the cluster head , wherein in case if cluster head is being compromised then whole WSN network CIA is on risk and this work is based on sensor nodes and how effective their grouping can be carry out. A basic encryption & decryption mechanism is being used for establishment of nodes and checking the genuineity if the same. Once formation of topology is formed then routing for the effective data communication can start and malicious nodes can be easily detected. This method is very effective in calculation of performance parameters like packet delivery ration wherein packets are only being transmitted to authentic node.

M.Conti et al., 2014 [13], study the behavior of different compromised and attack patterns. He proposed the model wherein node reliability is being calculated and these models are names as HIP (History-Information-Excahnge0-Protocol). This model is effective in some of the performance parameters like TP rate, detection rate.

III. PROPOSED METHOD

This section talks about the trust based framework system architecture, which can even handle unknown attacks, the system Architecture has different modules having different functions like Risk Analysis Module, which help, is picking up of right solution or IDS system. Data Aggregation module is responsible for formation of the group of network nodes and trust mechanism is responsible for establishing the calculation of right nodes for the communication and monitoring and IDM module is the intrusion detection management module which helps in attack identification and raising the alarm to stop the data transition or further analysis.

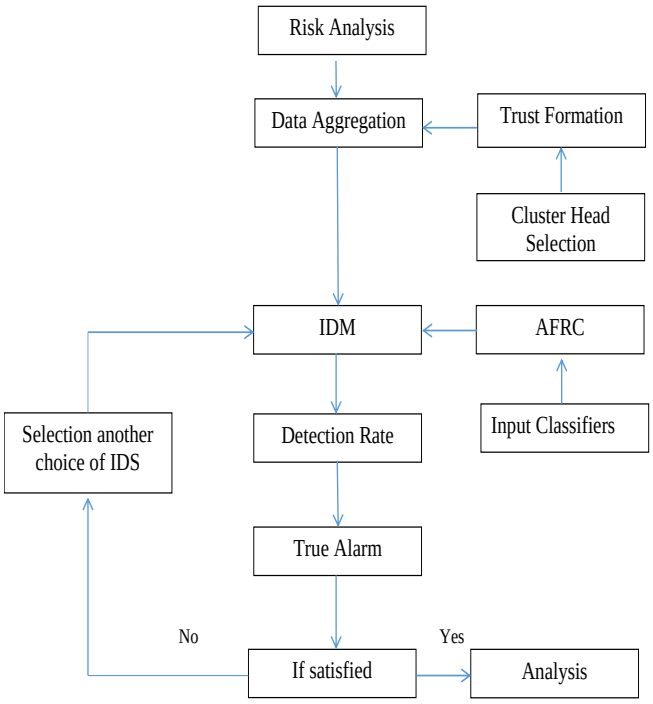

Fig. 2. Proposed System Architecture

IV. RESULTS AND DISCUSSIONS

In the beginning of experiments, to study the basic intrusion analysis, basic anomaly is being introduces in the WSN nodes and the behavior of performance parameters has been studies out to see the intrusion impact on the transmission. The following table represents the output as follows:

Table- I: Performance Analysis

Analysis Parameters	CW=8	CW=16	CW=24	CW=32
Packet Sent	1997	2004	2012	1993
Packet Received	1351	1072	1350	1345
Packet Delivery Function	67.65	53.49	67.1	67.49
Through-Put	1107.16	878.73	1106.05	1101.93
Mean Jitter	237.63	633.5	362.72	456.11
Current Jitter	210.5	587.35	340.56	435.62

The various comparisons can be describes as follows:

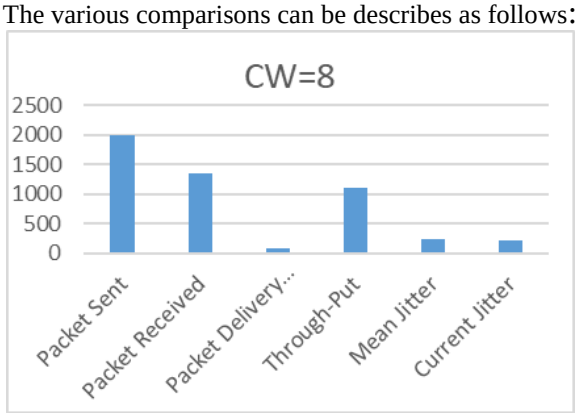

Fig. 3. Comparison for CW Value 8

For CW =16,

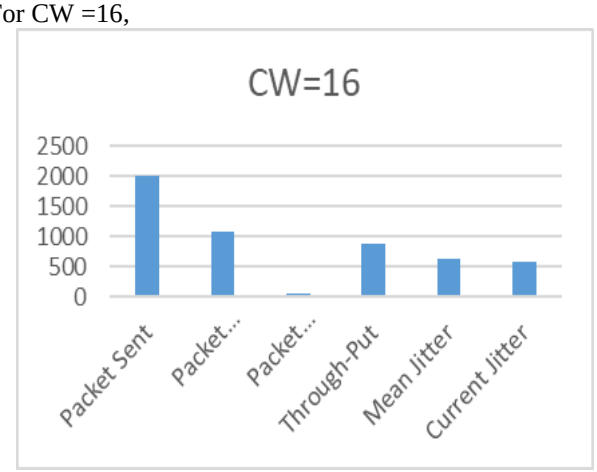

Fig. 4. Comparison for CW Value 16

For CW =24,

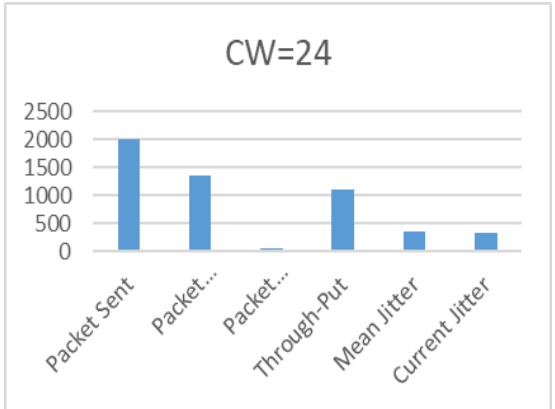

Fig. 5. Comparison for CW Value 24

For CW =32,

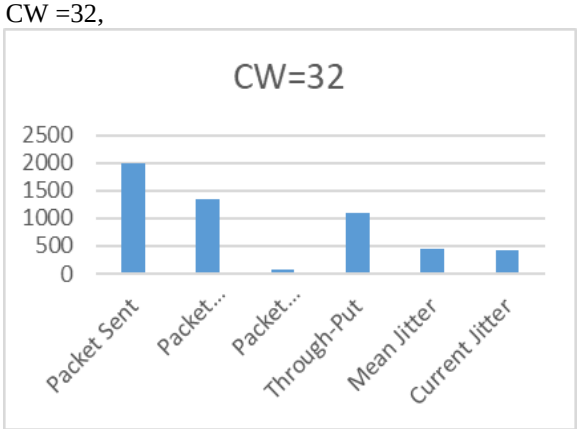

Fig. 6. Comparison for CW Value 32

These analyses are being carried out for the value of nodes =four, it can be derived from above results that performance is decreased for medium value of contention window i.e. 16.

In a sec number of bits transmitted in wireless network are known as throughput. In other word, throughput is also stated as data volume transferred or handled between nodes within time limit at certain amount. Throughput is usually measured in Kbps, Mbps.

For AFRC (Adaboost Fast Regression Classifier), with mechanism of machine learning, following are the results of implementation on Matlab:

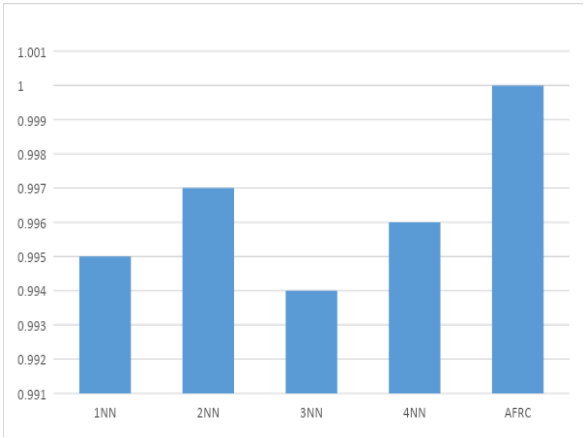

Fig. 7. Comparison of TP rate

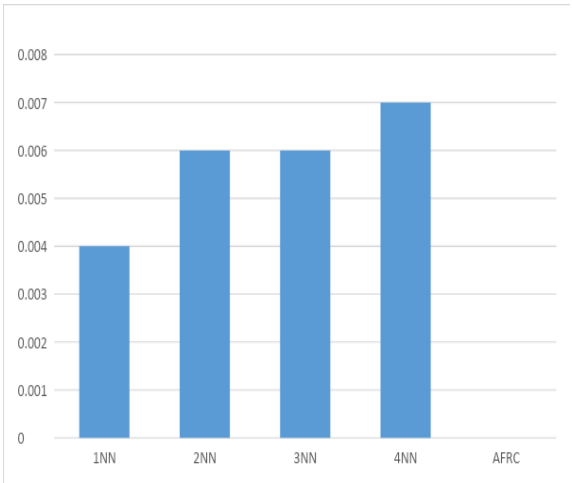

Fig. 8. Comparison of FP rate

V. CONCLUSIONS

In this paper, a system architecture is proposed, which is effective in handling unknown attack and can be further used for security vendors to upgrade the current architecture which can stop or prevent the attack to enter into the network

REFERENCES

1. Mihail Anghel, Andrei Racautanu "A note on different types of Ransomware attacks,"in *IACR,2019*.
2. Huang, J., Duan, Q., Zhao, Y., Zheng, Z., & Wang, W. (2016). Multicast routing for multimedia communications in the Internet of Things. IEEE Internet of Things Journal, 4(1), 215-224.
3. Danyang Q (2017),"Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network". IEEE Internet of Things Journal
4. Divya Pandey, Vandana Kushwaha (2017), "Experimental Tools and Techniques for Wireless Sensor Networks" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019.
5. Sattar B. Sadkhan, Hussein Mohammed Salman (2017), "Energy Efficient Malicious Node Detection System in Wireless Sensor Networks," International Conference on Current Research in Computer Science and Information Technology (ICCIT)
6. Meenakshi Panda and Mohan Khilar ,(2015)"Distributed Byzantine fault detection technique in wireless sensor networks based on hypothesis testing"ACM, Computers and Electrical EngineeringNovember 2015
7. Suraj Sharma,Deepak Puthal,Sanjay Kumar Jena and Albert Zomaya(2016),"Rendezvous based routing protocol for wireless sensor networks with mobile sink "The Journal of Supercomputing 73
8. Y R. Chapman, T S Durrani ,(2012),"IP protection of DSP algorithms for system on chip implementation",ACM IEEE Transactions on Signal Processing Volume 48, Issue 3
9. Vivek Katiyar, Prashant Kumar Narottam Chand (2011)" An Intelligent Transportation Systems Architecture using Wireless Sensor Networks." International Journal of Computer Applications (0975 – 8887) Volume 14– No.2, January 2011
10. David Martins & Herve Guyennet ,(2010)Wireless Sensor Network Attacks and Security Mechanisms, Proceedings of the 2010 13th International Conference on Network-Based Information SystemsSeptember,2010
11. Varsha Raghuwanshi and Umesh Lilhor (2016) Title. Neighbor Trust Algorithm (NTA) to Protect VANET from Denial of Service Attack (DoS), International Journal of Computer Applications Vol.140
12. S.G. Hymlin Rose, T. Jayasree. "Detection of jamming attack using timestamp for WSN" , Ad Hoc Networks, 2019
13. M.Conti et al., Title. Distributed detection of clone attacks in mobile WSNs, JOURNAL OF COMPUTER AND SYSTEM SCIENCES, 2014

AUTHORS PROFILE

Abhishek Jain received the Bachelor of technology in from Guru Jambheshwar University of Science & Technology, and Master of Technology from Maharshi Dayanand University Rohtak. Currently He is pursuing PhD in the Department of Computer Science and Engineering, Amity University Haryana, India. He is expert in cyber forensics and research interests include protection from cyber attacks

Dr. Vishal Jain is currently Associate Professor at Bhatati Vidyapeeth's Institute of Computer application & Management in Computer Science department.

Dr. Khushboo Tripathi is currently Assistant Professor at Amity University Haryana in Computer Science department.