iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

An approach of false misbehaviour removal in wireless sensor network using clonal selection algorithm and change point detection

Phiza Ambreen Khan[1], Mr.Kailash Patidar[2], Mr.Gajendra Singh[3]

[1]Research Scholar, Department of CSE (Software Engineering), SSSIST,Sehore
[2]Assistant Professor, Department of CSE, SSSIST,Sehore
3 Professor & Head, Department of CSE, SSSIST,Sehore

Abstract-Security of wireless sensor network becomes crucial key factor in the latest research available in the fast deployment of wireless sensor network. The time interval between an attack detection and corrective action taken by the administrator in a system is usually high and therefore, at the time the administrator notices an attack and takes some suitable action the damage was done by the attacker. Depending on this scenario the need for Intrusion Detection System which can not only detect various types of attacks but also be able to actively respond against malicious activities is required. Intrusion detection is a preemptive approach in a system security which is used to identify malicious activities and respond quickly to mitigate anomalous behaviour.

In this research paper we actively proposed a new and efficient approach in intrusion detection by analyzing past approaches proposed in this research area. We define the basics of intrusion detection in wireless network by describing the varieties of attacks and state the motivation for intrusion detection in wireless network. In this paper, we proposes an IDS which is based on watchdog monitoring technique and is able to detect selective forwarding attacks and also able to eliminate the postulates of watchdog algorithm by using change point detection algorithm.

Keyword- WSN, IDS, attacks, Watchdog Monitoring Techniques

I. INTRODUCTION

The wireless sensor networks (WSNs) are often deployed in physically insecure environment where we can hardly prevent attackers from the physical access to the devices. Since making nodes resistant to physical tampering would make them much more expensive, we have to think that an attacker may capture the nodes and retrieve the cryptographic material via physical tampering [1, 2]. A wireless IDS may aid within the detection of a variety of attacks. Not solely will a wireless IDS Sight knave WAPS, determine non-encrypted 802.11 traffic, associate degree facilitate isolate an attacker's physical location, as mentioned earlier - a wireless IDS will sight several of the quality (and not-so standard) wireless attacks and probes still. In an attempt to spot potential WAP targets, hackers ordinarily use scanning computer code. Utilized in conjunction with a worldwide Positioning System (GPS) these scans not solely find WAPs.

However additionally log their geographical coordinates. These tools became thus well-liked that they're square measure websites dedicated to mapping the world's WAP earth science. A wireless IDS will cite these and other scans, serving two to boost awareness of the threats to the wireless fidelity.

ISSN: 2321-9653

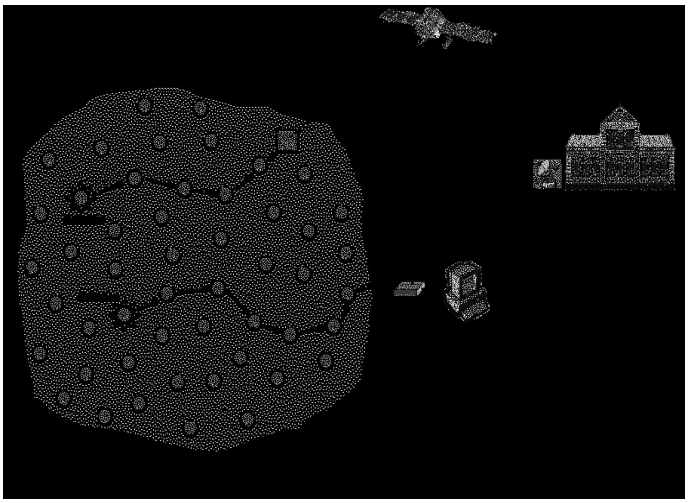


Figure 1.Wireless Sensor Network

A wireless network could be a wireless network consisting of spatially distributed autonomous devices exploitation sensors to hand in glove monitor physical or environmental conditions, like motion, temperature, pressure, sound, vibration, , or pollutants, at completely different locations the event of wireless networks was originally driven by military applications like field of battle police investigation. However, wireless networks square measure currently utilized in several civilian application areas, as well as setting and surround observance, control, home automation, and health care applications.

Wireless sensor network refers to a system that consists of variety of inexpensive, resource restricted detector nodes to sense vital information associated with setting and to transmit it to sink node that gives entrance way practicality to a different network, or associate degree access purpose for human interface. Wireless sensor network could be a speedily growing space as new technologies square measure rising, new applications square measure being developed, like traffic, setting observance, healthcare, military applications, home automation. A wireless network is susceptible to numerous attacks like jam, battery avoidance, routing cycle, Sybil, cloning. Thanks to limitation of computation, memory and power resource of detector nodes, advanced security mechanism can't be enforced in Wireless sensor network. So energy-efficient security implementation is a very important demand for Wireless network. To protect Wireless network against completely different varieties of vulnerabilities, preventive mechanisms like cryptography and authentication will be applied to stop some sorts of attacks.

This sort of preventive mechanisms fashioned the primary defence line for Wireless network. However, some attacks like wormholes, sinkhole, couldn't be detected exploitation this sort of preventive mechanisms. Additionally, these mechanisms square measures solely effective to stop from outside attacks and didn't guarantee the interference of intruders from within the network (Silva et al., 2005). Due to that, it's necessary to use some mechanisms of intrusion detection. Intrusion Detection Systems (IDS) square measure thought of to act because the second defence line against network attacks that preventive mechanisms fail to deal with (Silva et al., 2005). Associate degree Intrusion detection system is outlined in (Debar et al., 1999) .A system that dynamically monitors the events going down on a system associate degree decides whether or not these events square measure symptoms of an attack or represent a legitimate use of the system. However, there square measure several challenges posed against the appliance of the IDS for Wireless network. These challenges square measure thanks to the dearth of resources like, energy, process and storage. Wireless networks square measure assortment of nodes wherever every node has its own detector, processor, transmitter and receiver and such sensors sometimes square measure low price devices that perform a selected variety of sensing task. Being of low price such sensors square measure deployed densely throughout the world to watch specific event.

The Wireless network largely operates publicly and uncontrolled space gives a chance to intruder to trespass the safety of a application. Today Intrusion used as a security resolution in a much wired sensor network within the type of software/ hardware by that one will sight unwanted services happening the system by approach of enhanced/abnormal network activity and determine suspicious patterns that will indicate whether or not the network/system is beneath attack? For Wireless sensor network many schemes were projected however they need restricted options like solely concern to attacks on a specific layer.

ISSN: 2321-9653

II. Fundamentals of Intrusion Detection in Wireless Sensor Network

We introduce the basics of the intrusion detection in Wireless network, which has the definition of the intrusion, kinds of intrusions/attacks in Wireless network, the motivation and want for intrusion detection and therefore the challenges of developing an honest candidate intrusion detection theme for Wireless network. The definition of the Intrusion Attack: Heady (1990) defines the intrusion as any set of actions that try to compromise the most parts of the safety system: the integrity, confidentiality or handiness of a resource. Within the same work, the interloper so was outlined as a personal or cluster of people WHO take the action within the intrusion.

Zamboni (2001)] adds the statement of success or failures of those actions thus it additionally refers to the attacks against the pc system. Within the theme of wireless detector network, the conception stills constant since the intrusion additionally target any of the parts mentioned on top of. The character of Wireless network and its special characteristics just like the harsh readying, energy constraints and therefore the media of communication makes them terribly liable to the intrusions quite different networks.

2.1Types of Intrusion Detection System

There are two types of approaches based on the detection technique in wireless sensor network: Misuse Detection also referred to as Signature based Intrusion Detection (SID) and Anomaly based Intrusion Detection (AID). In SID detection, each network traffic record is recognized as either normal or one of many predefined intrusion types. In contrast, anomaly detection amounts to training models for learning normal traffic behaviour and then classifying, as intrusions, any network behaviour that considerably deviates from the known normal network traffic patterns.

Intrusion signatures have been characterized as a string, event sequences, graphs, and intrusion scenarios (consisting of target states, event sequences, and their preconditions). FSM (finite-state-machine), colored Petri Nets, associate rules and production rules of expert systems have been used to represent and recognize intrusion signatures. Intrusion signatures are either physically encoded or manually learned through data mining. But, signature recognition techniques have a limitation in that they cannot detect original intrusions whose signatures are unknown.

2.2 Types of attacks in Wireless network:

- Outsider versus business executive attacks supported the node that's launching the attack, if it happiness to the network thus it's thought-about as business executive attack, otherwise it's thought-about as outsider attack.

- Passive versus active attacks supported the impact that results from AN attack. Passive attacks simply monitor or pay attention to the info packets, whereas the active attacks do modify the info streams or according false alarms to the bottom station.

- Mote-class versus laptop-class attacks supported the potential of the wrongdoer in compromising the network. In mote-class attacks, some nodes with an analogous capability to the network nodes are used as attackers, whereas in laptop-class, uses powerful devices like laptops with higher transmission varies, processing power and energy to compromise the network.

III. Watchdog Mechanism

Watchdog is a monitoring mechanism introduced to identify the misbehaving nodes in the network [1][6].In this approach each sensor node has its own watchdog that monitors and records its one hop neighbour's behaviour such as packet transmission. When sending node A sends a packet to its next node B, the watchdog in A verifies whether B forwards the packet to the next node or not by using its overhearing ability within its transceiver range But watchdog has the limitation [2] of not being able to detect the misbehaving nodes in the following conditions.

- **Ambiguous collision**: Consider A forwards a packet to B and overhears whether b is forwarding it or not. When B forwards it to C, A may not overhear this transmission if other neighbours of A send packets to it at the same time. This may mislead A to conclude that B is malicious but this may not be correct.

- **Receiver collision**: Collision may occur at the receiver side also (i.e.) C may not receive the packet. A can overhear that B has forwarded the packet, but it cannot tell whether C has received the packet.

- **Limited transmission power**: If B can adjust its transmission power such that A can overhear but C does not receive, then B can drop packets and prove its trustworthiness.

- **False misbehaviour**: A malicious node intentionally reports that other nodes are misbehaving. A can report that B is dropping packets although B is not. In this case A's neighbour node S which cannot\ communicate directly with B, can consider B as malicious.

- **Partial dropping**: Instead of dropping all packets, B can drop only some packets such that the failure tally will not exceed the detection threshold of A's watchdog.

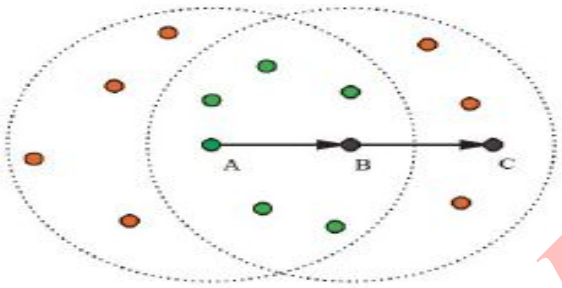


Figure 2: Watchdog Mechanism in Wireless Sensor Network

IV. Related Work

Forootaninia [1] et.al proposed "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks", they focused on to resolve the ambiguous collision of packets in watchdog mechanism. There are certain problems existing in watchdog have been resolved but still one of the problems in watchdog, the malicious node detection due to ambiguous collision of packets has not been solved.Youngho Cho[2] et.al proposed " Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks", they focused on overhearing ability of the sender sensor node within its transceiver range But watchdog has the limitation of not being able to detect the misbehaving nodes in the following conditions.

Yuxin Mao [3] et.al proposed "A Secure Mechanism for Data Collection in Wireless Sensor Networks", the objective is to improve the existing watchdog monitoring system by implementing the change point detection algorithm in it, there by detecting the exact malicious node in the network. Lei Huang [4] et.al proposed Extended Watchdog Mechanism for Wireless Sensor", they focused on to overcome the limitations of watchdog monitoring system which was improved by adding a threshold mechanism .In this mechanism sensor node stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match.Abror Abduvaliyev [5] et.al proposed "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", in this mechanism signal strength was proposed to detect the malicious nodes in a network. The idea was to compare the signal strength of reception with its expected value. A signal is only detected by a receiving node if the received signal power is equal or greater than the received signal power threshold. If the signal power received is less than the threshold then the particular node is suspected to be malicious.

CE Loo [6] et.al proposed "Intrusion Detection for Routing Attacks in Sensor Networks", The detecting technology and sensing technology combined with processing power and wireless communication makes it lucrative for being adopted in great quantity in future. The wireless communication technology is also looking for various types of security threats. Sergio[7] et.al proposed "Mitigating routing misbehaviour in mobile adhoc networks", they focused on to design routing protocol for WSN is very much challenging manner and shows that the protocols have a high diversity to match up with requirements of the application scenarios.A.Babu[8] et.al proposed "False Misbehaviour Elimination In Watchdog Monitoring System Using Change Point In A Wireless Sensor Network", they focused on both the possibilities of detecting the malicious node and also declaring a true node to be malicious. By using the proposed algorithm the exact malicious node is found to be identified in all the rounds. The malicious node detected by the proposed algorithm is found to be accurate irrespective of the number of rounds conducted.

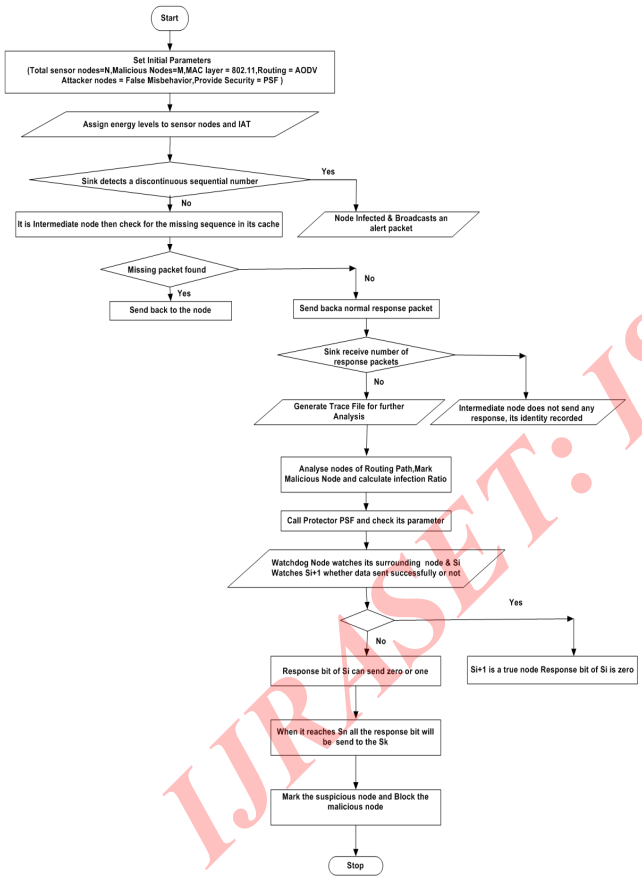
ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

V. PROPOSED APPROACH

Watchdog algorithm is in existence is unable to catch the misbehaving sensors due to which network traffic is being upset. Our goal is to create an IDS such that the throughput of the system must be efficiently increased and PDR must be improved. The constraint of the system with our protection scheme must be comparable with the system without having any attack. We implement two algorithms simultaneously to detect the nodes which acting as true node and fake other true nodes to be misbehaving. The proposed detection Algorithms are discussed below.

Flow Chart of Proposed Algorithm



In a typical WSN every node is crucial for proper communication, so we implemented the algorithm which is specially designed for these issue resolving detection and protection false misbehaviour attack under sensor network, First we have to initialize the variables and check the intrusion type by the means of behaviour, after detection of attacking node we apply the protection scheme in which we detect the malicious node and then sends the alert message to the network. The malicious node is then blocked by selecting alternative route for sending the data. Algorithm to implement proposed approach with least increase in computational complexity is given below:

Proposed Algorithm for malicious node detection and false behaviour elimination in WSN:

Input: T =A topology in which m number of malicious node present in a set of n number of sensor nodes.

Output: O = set of clusters which are having watchdog nodes used to find malicious nodes Set initial parameter of network

Step 1: Mobile Sensor Node's = N; MAC layer = 802.11, Routing = AODV, Attacker nodes = False Misbehaviour,

Provide Security = PSF (Protection scheme for false misbehaviour), Inter Arrival Time = IAT (Control Rate at Different Time) //Attacker launches false misbehaviour

Attacker-node
(capture vulnerable node information && send =false alarm packet && rate = 232*0.1s)

If (Sink detects a discontinuous sequential number)

{

Infected;

Broadcasts an alert packet;

}

Step 2 : For (Intermediate node check for the missing sequence in its cache)

{

If

{

Missing packet found;

Send back to the node;

}

Else

{

Sends back a normal response packet;

}

}

Step 3 : If (Sink receive number of response packets)

{

Intermediate node does not send any response, its identity recorded;

}

Step 4 : Generate trace file for further analysis

Step 5 : Do (analysis trace for detection)

{

Analyse the nodes of the routing path, Mark the malicious node;

Find infection ratio;

}

Step 6: Call protector PSF

While (PSF-Check vulnerable node && total packet receives && rate && sender)

{

For (Si Watches Si+1 whether data sent successfully or not)

{

At the same time S0 sends the data to the Si;

If

{

Si+1 is a true node;

Response bit of Si is zero; }

Else

Response bit of Si can send zero or one;

}

Step 7 : Do (When it reaches S_n all the response bit will be send to the S_k)

{

Suspicious point = previous status bit as 0 or -1 transit to 1;

Mark the suspicious node and Block the malicious node;

}

VI. CONCLUSIONS

Here we are analysing the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range).The analytical model for intrusion detection allows us to analytically formulate intrusion detection possibility within a certain intrusion distance under various application scenarios. Once we find the intruders than technique is used to stop intruders is RF jamming through salutatory-style channels i.e. changing by spacing a channel. Our Intrusion Detection System also implement in internet application and parallel computer interconnection network.

ACKNOWLEDGMENT

We would like to express our gratitude to Mr.Gajendra Singh and Kailash Patidar for all their hard work in completion of this work. We also extend our gratitude towards Principal, SSSIST, Sehore for his valuable guidance in all hard times. Finally we thank our institution for providing a platform for new innovations.The heading of the Acknowledgment section and the References section must not be numbered.

REFERENCES

[1] An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks A. Forootaninia1 and M. B. Ghaznavi-Ghoushchi,International Journal of Network Security & Its Applications (IJNSA), 2012

[2] Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks Youngho Cho and Gang Qu, IEEE Symposium on Security and Privacy Workshops ,2012

[3] A Secure Mechanism for Data Collection in Wireless Sensor Networks Yuxin Mao, School of Computer and Information Engineering, Zhejiang Gongshang University, Applied Mathematics & Information Sciences – An International Journal, 2010.

[4] Extended Watchdog Mechanism for Wireless Sensor Networks Lei Huang , Lixiang Liu, Journal of Information and Computing Science, 2007

[5] Abror Abduvaliyev, Al-Sakib Khan Pathan, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks" in IEEE Communications Surveys & Tutorials,Vol. 15, No. 3, Third Quarter 2013

[6] CE. Loo, MY. Ng, C. Leckie, and M. Palaniswami, Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, vol. 2,pp. 313-332, 2006.

[7] Sergio Marti, T. J. Giuli, Kevin Lai, "Mitigating routing misbehaviour in mobile adhoc networks" in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255–265, New York, NY, USA, 2000. ACM.

[8] A.Babu Karuppiah, T.Meenakshi, "False Misbehaviour Elimination In Watchdog Monitoring System Using Change Point In A Wireless Sensor Network" in International Journal of Graduate Research in Engineering and Technology (GRET),2012.

[9] Tapas Badal and Dipti Verma, "A Modular Approach for Intrusion Detection System in Wireless Networks", International Journal of Advances in Computer Networks and Security, pp. 57-61, May 2012.

[10] Chilakalapudi Meher Babu, Dr. Ujwal A. Lanjewar, Chinta Naga Manisha "Network Intrusion Detection System on Wire Less Mobile Ad hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, pp. 1495-1500, March 2013.

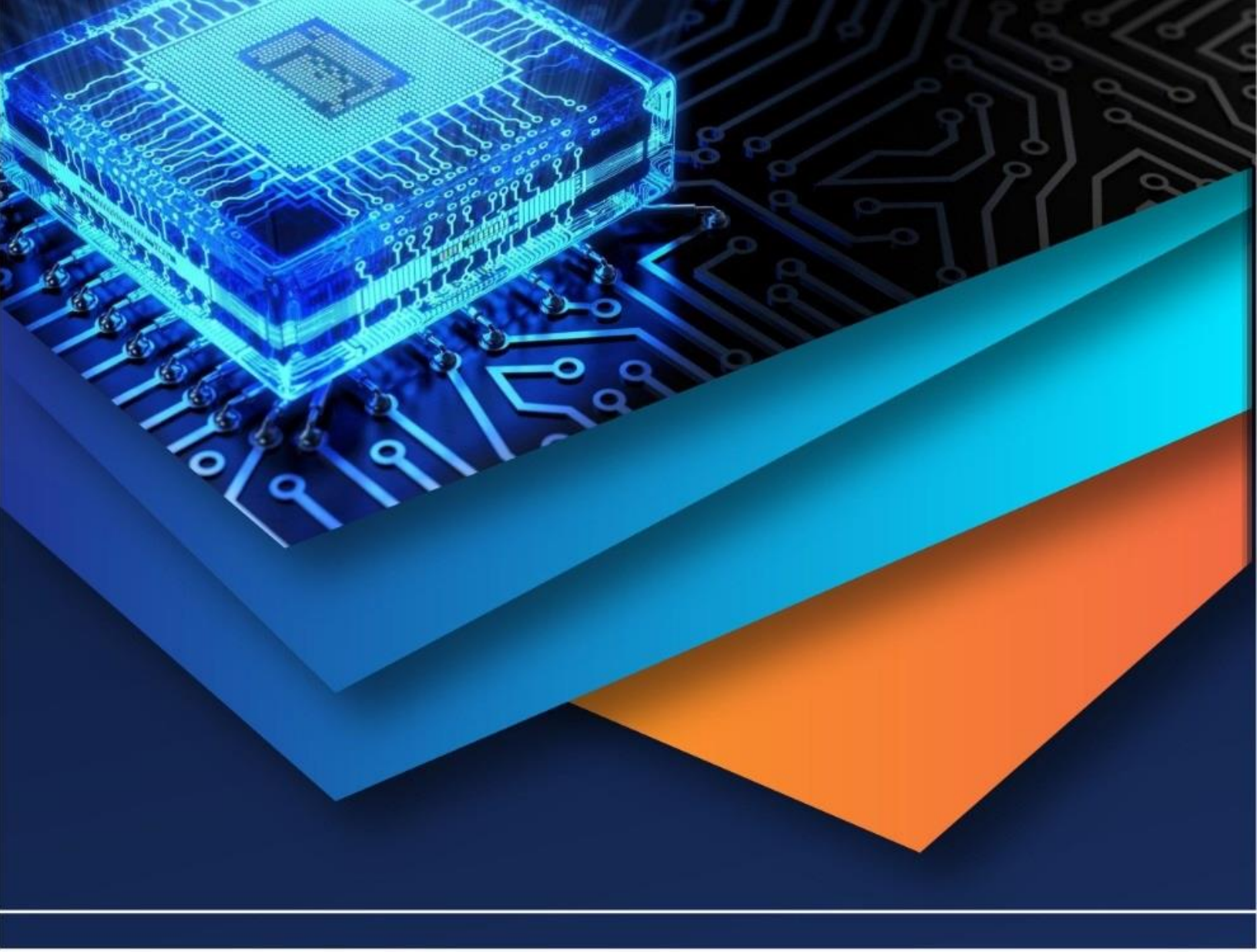
[11] Xie, M., S. Han, B. Tian and S. Parvin, "Anomaly detection in wireless sensor networks: A survey" Journal Network Computer Application (JNCA), 1302-1325.2011.03.004, 2011.

[12] Stetsko, A., L. Folkman and V. Matyas, "Neighbor-based intrusion detection for wireless sensor networks", Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), Sept. 20-25, IEEE Xplore Press, Valencia, pp: 420-425. DOI: 10.1109/ICWMC.2010.61, 2010.

[13] Lemos, M.V.D.S., L.B. Leal and R.H. Filho, "A new collaborative approach for intrusion detection system on wireless sensor networks", Novel Algorithms Techniques Telecommunication. Network DOI: 10.1007/978-90-481-3662-9_41, 2010.

[14] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci and Edward Knightly, "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks", IEEE/ACM Transactions On Networking, Vol. 17, No. 1, , pp. 26-39, February 2009.

[15] Erik Kline, Alexander Afanasyev, Peter Reiher.: "Shield: DoS Filtering Using Traffic Deflecting", 19th IEEE International Conference on Network Protocols, pp. 37-42, 2011..



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY