iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XI **Month of publication:** November 2020

DOI: https://doi.org/10.22214/ijraset.2020.32365

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

Detection of Black Hole Attack using Secured AODV Routing Protocol in WSN

Miss. Chetna N. Pushpatode[1], Dr. Mrs. S.V. Sankpal[2]
[1]*M. tech., Department of Electronics & Telecommunications Engineering, D.Y Patil College of Engineering & Technology, Kolhapur*
[2]*Associate Professor, Department of Electronics & Telecommunications Engineering, D.Y Patil College of Engineering & Technology, Kolhapur*

Abstract: ***Wireless Sensor Network (WSN) is an infrastructure less that has no central administration and limited capabilities in term of energy, power consumption, and data storage capacity. Furthermore, WSNs are key technologies for IoT. The routing protocol is one of the most concerned areas in WSNs which is responsible for maintaining the routes in such that network. In this paper, we aim to enhance the security of WSN routing protocol. Our contribution is modified Ad Hoc On-Demand Distance Vector (AODV) routing protocol by building a security layer that utilizes Paillier homomorphic cryptographic mechanism; to protect forwarding packet data and routing during the communication and deliver data integrity and confidentiality The simulation is carried on NS-2 and the results of the proposed scheme are compared to the fundamental AODV routing protocol, these results are examined on various network performance metrices such as packet delivery ratio, throughput and end-to-end delay.***

Keywords: WSN, AODV, Secure routing protocol, Paillier cryptosystem, NS2

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensor to monitor physical or environmental condition such as temperature, sound, vibration, pressure, motion or pollutants in different location. A simple change in node status leads to the unpredictable change in topology. Initially, WSN was evolved basically for military application which was a very challenging job. Even today, when civilian applications have been recognized, it is the major source of information for military in remote areas [13]. Because of the unique requirements of the routing, WSNs need specific routing algorithm and naturally, there is always a demand of routing algorithms which are energy efficient, optimized, data centric and secure. Due to the wireless and distributed nature of WSNs, these are less protective and hence more prone to security attacks and also in WSN the quick deployment of the nodes to establish a route is the important issue. Black hole attack is one of the serve security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on- demand routing protocols such as AODV.

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is most commonly used routing protocol in WSN [11]. It is a reactive routing protocol uses on-demand approach to find routes, so, nodes will send the control data only when is necessary. The black-hole attack is considered one of the most widespread active attacks that degrade the performance and reliability of the network as a result of dropping all incoming packets by the malicious node. In black hole attack a malicious node sends the RREP (Route Reply) message to the source node as a shortest path to the destination node then the sender node sends a data packet to the malicious node in the network. Finally, the malicious node drops the entire data packet instead of forward it to the destination node. The conceptual diagram of black hole attack is shown in figure 1. The packets sent by node 1 which is source node destined for node 2 are consumed by node B which is black hole node.

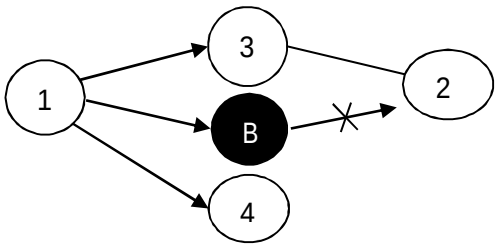


Figure 1: Black hole node present in WSN consuming all packets destined for other node

©IJRASET: All Rights are Reserved

Black hole node aims to fool every node in the network that wants to communicate with another node by pretending that it always has the best path to the destination node. AODV protocol that has no techniques to detect and neutralize the black-hole node in the network [3]. Therefore, this work proposes a technique to enhance the security of AODV routing protocol by detecting and preventing the threat of black hole attacks.

II. RELEVANCE

In the basic mechanism of AODV, when a source node has a data packet addressed to a destination node, the source node checks its routing table first which contains the next hop to use to reach the destination node. However, if a valid route is found, the source node sends the data packet to the next hop to forward it to the target node. If no route is found, the source node starts route discovery process to find new route to the destination. The route discovery phase is initiated by broadcasting a route request packet (RREQ). When an intermediate node receives a RREQ, it either forwards it or generates a route reply (RREP) packet and it does not forward the RREQ any further if it has a valid route to the destination. Within this route discovery process, only the destination node itself or an intermediate node that has a valid route to the destination are allowed to send a RREP to the RREQ's source node, hence, RREQ messages may not necessarily reach the destination node. This enables faster replies and limits the flooding of RREQ's. This process continues until a RREP message from the destination node that has a fresh route to the destination node is received by the source node. In this rerouting the network traffic through a specific node controlled by the attacker is the main goal of black hole attack [4]. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh route to the intended destination. Malicious nodes respond immediately to the source node without even checking its routing table by claiming that it has the freshest and the shortest route to the destination on the route reply packet sent back to the source node. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and accepts the path through the malicious node to route data packets. The data packets will be dropped now by the malicious node instead of forwarding them to the destination as the protocol requires. Imposing security in WSN is a very challenging and hot topic of research science last two decades because of its wide applicability in applications like defense. Number of efforts has been made in this direction. Through the literature survey, it is motivated to enhance security of AODV routing protocol in WSN by improving the life of network and throughput.

III. PROPOSED WORK

This work proposes the development of an algorithm which can detect and avoid black hole in wireless sensor network while routing the packets from source sensor node to destination node. The RREQ and RREP packets during route establishment process of AODV protocol are to be modified for security against black hole attack and preventing the consumption of packets.

A. Objectives

The objectives of proposed work are as follows:

1) To develop the method for bypassing black hole attacking node in the wireless sensor network.
2) To modify field contents in RREQ packet of AODV at source node.
3) To verify field contents using Paillier security algorithm and then forward RREQ at destination.

B. Methodology

Selecting an appropriate, proven methodology is important step in any research endeavor. To evaluate the performance of proposed work we will design a simulation model. The design steps in simulation model are as below:
The working of proposed work is explained below:

1) *Step 1:* Before sending the RREQ, the source node stores the intended destination address and replace it by its hash value in the RREQ packet and broadcast it.
2) *Step 2:* If an intermediate node receives the RREQ, it sends back a RREP after setting the real address of the destination node only if it is the destination by comparing the hash value with the destination node address set on the RREQ packet. Otherwise, the intermediate node forwards the RREQ packet.
3) *Step 3:* If RREP's source address is not expected, it will be rejected. Since, only malicious nodes reply for non-existing target address.
4) *Step 4:* If the RREP is valid then compare its sequence number to calculate threshold: If RREP's sequence number <= threshold then the source node accepts the RREP and update its routing table, otherwise, the RREP will be rejected. The threshold is calculated as following:

Threshold = AVERAGE (all received RREP's sequence number) + MIN (all received RREP's sequence number)

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

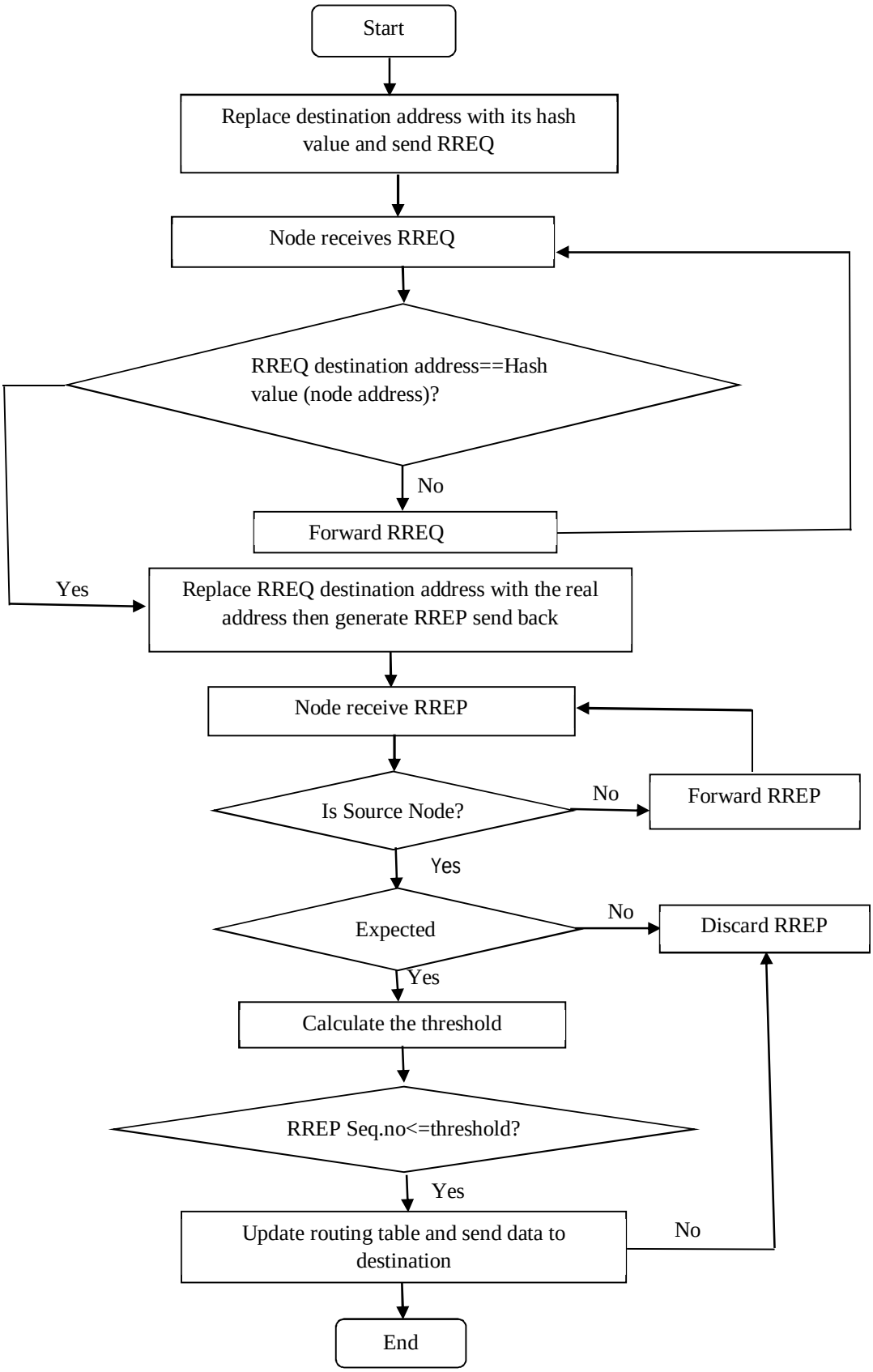


Figure 2: Flow graph of proposed work

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

In the proposed strategy, Cyclic Redundancy Check 32 bits (CRC-32) is used as hash function [10]. The change to be made on the AODV message formats will be the RREQ message format. In fact, the destination address field will be replaced by its hash value which have the same length [4] that keeps the RREQ message format the same and it will not result any extra overhead and will not change the packet size.

C. Algorithm

This work proposes enhancement in security AODV routing protocol in WSN routing by using paillier algorithm. Paillier is a homomorphic cryptography. Paillier algorithm involved key generation, encryption and decryption [13].

Algorithm Paillier Cryptography

1) Key Generation

Generation two large prime numbers p and q randomly and independently of each other

$n = p \times q$

$\lambda = lcm\ (p-1, q-1)$ (λ is Carmichaels function)

$L\ (u) = u-1/N$

$\mu = L(g\lambda MODn^2)^{-1}\ MOD^n$

Public key $\longleftarrow$ (n, g)

Private key $\longleftarrow$ (L, μ)

2) Encryption

$C = g^m.r^n\ MODn^2$

3) Decryption

$D = L\ (c\ \lambda(MODn^2)).\ \mu(MODn)$

D. Evaluation Metrics

The performance of proposed work will be evaluated by simulation model

1) Simulation tool :- NS2
2) Simulation area (km x km) :- 2.5 x 2.5
3) Routing Protocol :- AODV
4) Size of the Network :- 40-50 nodes
5) Malicious Node :- 1

E. Performance Parameters

The proposed work consists of black hole prevention attack and hence it is desirable to measure the packet delivery ratio at the actual destination node in WSN. Along with this, throughput and end to end delay parameters are to be measured to verify the impact of black hole prevention and performance of WSN.

1) Packet delivery ratio: - It is number of successful packets received/ Number of packets sent
2) Throughput: - It is number of packets received per second or number of kilobytes received per second
3) End to end delay: - It is delay of each packet to reach at the destination from sent time.

IV. SIMULATION RESULTS AND DISCUSSION

In order to test and confirm the performance of proposed strategy, we have implemented the solution in a simulation environment which generates the same behavior in the real ad-hoc networks. To evaluate the proposed solution, we relied on the NS2 simulator with the simulation parameters chosen as mentioned above. In the further study, we will used Network Animator (NAM) for simulation process and analysis.

To evaluate the efficiency of the proposed method we analyzed on the basis of three performance metrics as described above. In our simulation, the proposed scheme and are simulated under an intelligent Black Hole attack and the results are compared with the fundamental AODV routing protocol. As shown in figure 3, the packet delivery ratio of the proposed scheme is highly better than proposed solution in earlier report [14], moreover our proposed scheme has a PDR nearly equal to the fundamental AODV without attack,

©IJRASET: All Rights are Reserved

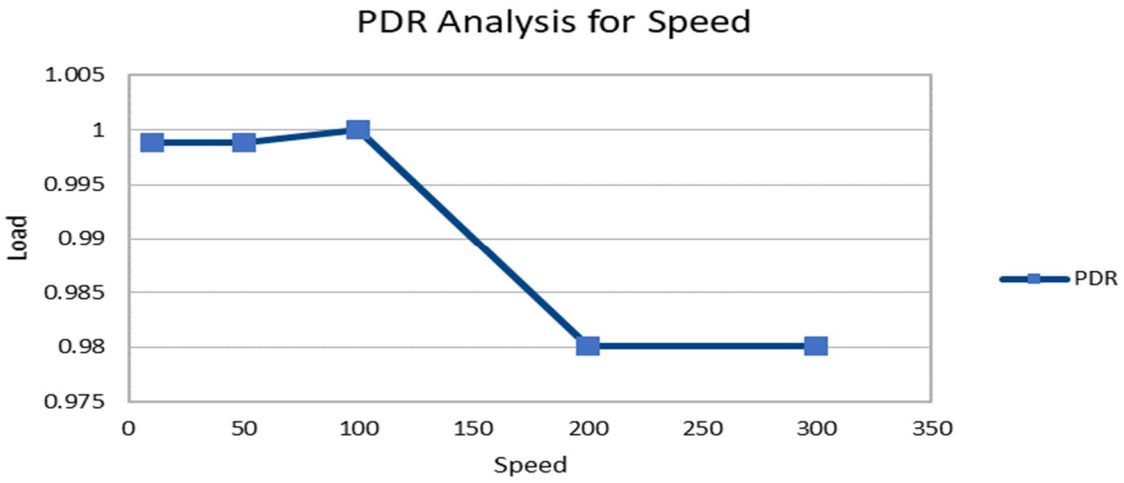


Figure 3. Impact of Node Numbers on PDR

V. CONCLUSION

Here we discussed intelligent black hole attack and prevented via our proposed strategy. The simulation result proves the efficiency of the proposed solution since it has the ability to ensure high packet delivery ratio and compare to the fundamental AODV.

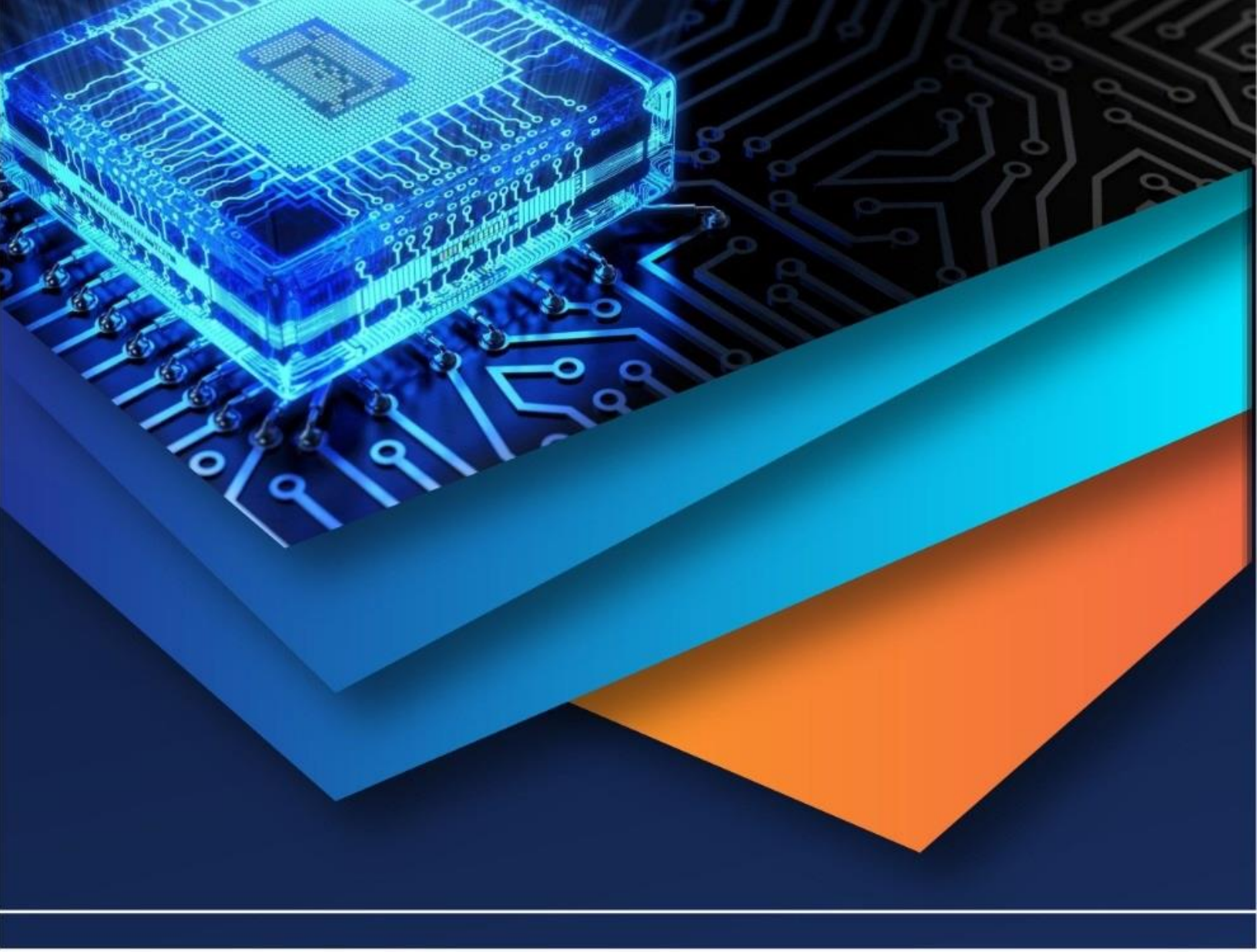
VI. ACKNOWLEDGEMENTS

We would like to thanks to all those who help us to complete this research paper.

REFERENCES

[1] X. Liu, X. Zhang, N. Guizani, J. Lu, Q. Zhu, X. Du, "TLTD: A Testing Framework for Learning-Based IoT Traffic Detection Systems", Sensors 2018, 18, 2630; doi:10.3390/s18082630
[2] J. M. Blythe and S. D. Johnson, "The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-7. doi: 10.1049/cp.2018.0004.
[3] D. Dinesh, A. Kumar, and R. Mahajan, "Integrated Approach to Find Trusted Path under Black hole problem in Ad-hoc networks using Digital Signature and Back Trace-AODV," Int. J. Adv. Res. Compute. Sci., 2017, vol. 8, no. 5.
[4] M. Sathish, K. Arumugam, S. N. Pari and V. S. Harikrishnan "Detection of single and collaborative black hole attack in MANET, "International conference on wireless communications, signal processing and networking (Wisp NET), Chennai, 2016, pp. 2040-2044.
[5] P. S. Hiremath, and T. Anuradha "Adaptive Method for Detection and Prevention of cooperative black hole attack in MANETs", International journal of electrical and electronics and data communication, 2015, Volume-3, Issue-4, pp.1-7.
[6] S. Singh, P. Kumari and S. Agrawal, "Comparative Analysis of Various Routing Protocols in VANET, "Fifth International conference on advanced computing & communication technologies, Haryana, 2015, pp. 315-319.
[7] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni., "A reputation system for detection of black hole attack in vehicular networking," *International conference on cyber security of smart cities, industrial control system and communications (SSIC)*, Shanghai, 2015, pp. 1-5.
[8] E. C. Eze., S Zhang. and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," 2014 20th International conference on automation and computing, Cranfield, 2014, pp. 176-181.
[9] C.E Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing", Proceedings of IEEE workshop on mobile computing systems and applications 1999, Feb 1999, pp.90-100.
[10] Cyclic Redundancy Check (CRC) RFC. Available online: https://tools.ietf.org/htm/rfc 3385.
[11] S. Saleem, S. Ullah, H. S. Yo, On the Security issues in wireless body area networks 2009, International Journal of Digital Content Technology and its Applications Vol.3, No. 3, pp.178-183.
[12] A. S. Sastry, S. Sulthana, S. Vagdevi, Security threats in wireless sensor networks in each layer, 2013, Int. J. Advanced Networking and Applications, Vol.04 Issue: 04 pp.1657-1661.
[13] R. Harerimana, S.-Y. Tan, and W.-C. Yau, "A Java implementation of paillier homomorphic encryption scheme," in Information and Communication Technology (ICoIC7), 2017 5th International Conference on, 2017, pp. 1–6.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)