JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 159-168
https://publishoa.com
ISSN: 1309-3452

A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network

Dr. K. Madhuri, Professor, Neil Gogte Institute of Technology, Hyderabad, India

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

Abstract:
Recently, wireless sensor networks (WSNs) have received much attention by researchers because of their lower cost of deployment and easier to use. These networks are more vulnerable towards security attacks due to the lack of centralized management. The packet drop attack is one of the significant attacks that involve dropping of packets due to malicious compromised node. Different methods are proposed for detection of packet drop attack in WSNs, but these techniques are not providing the feasibility to isolate or stop these attacks' occurrence. The important mechanism is the reputation systems' utilization for WSNs. Each node allocates with reputation that determines with a node behaviour using a reputation system. The trustworthy nodes' have been detected using these reputation systems to perform data forwarding process. However, the effective way to monitor the data forwarding behaviour of a node is the nodes' monitoring in a promiscuous mode. A new intrusion detection system was proposed in this paper as a methodology of certificate revocation for effective operation and distribution of keys among nodes. The malicious nodes' keys have been revoked with the introduction of a certificate revocation method. As the malicious nodes are not having valid keys, they couldn't contact to the remaining nodes. The proposed mechanism simulates using the Network Simulator-2 for different scenarios that enhances network security by comparing with other traditional security algorithms.

Keywords: Black hole attack, Malicious Nodes, Packet Drop Nodes, Energy-Efficiency, Wireless Sensor Networks, IDS-SCRT.

I. INTRODUCTION

WSNs are having numerous applications for different fields like environment monitoring, battlefield observation, and health monitoring due to their advancements and developments [1]. WSNs have been deployed in different fields of observation as they include the features like self-organization, data-centric, and dynamic nature. They have sensor nodes that support for communication process in different high-level applications. WSNs include various sensor nodes that could monitor the changes of environmental conditions without depending on the particular infrastructure. Various research efforts have been focused on efficient deployment of WSNs for different applications that couldn't fulfill based on its general-purpose [2]. In some particular applications, different network parameters, such as transmission range, communication, density of nodes, and sensing range are considered for designing phase of a network. For this, it's needed to assess these parameters' effect on the network performance.

WSNs with wider usage is faced various security problems [3-5]. They have been suffered from various attacks because of the transmission medium's open and distributed nature. The attacks are included hijack attacks, tampering attacks, hello-flood attacks, blackhole attacks, selective forwarding, sinkhole, and Denial of Service attacks [6-7]. These attacks couldn't be resolved by prevention-based technologies and required to be incorporated the detection-based methods. By comparing with ad-hoc networks, WSNs has been included a challenging issue as routing owing to the constrained battery resources [8]. The routing method is needed to be efficient for resource utilization as sensor nodes of WSNs have limited processing, bandwidth, and memory capabilities [9].

The sensor network has an ability of communication, processing, and sensing for observing and reacting to the events of a particular environment. It contains tens to thousands of sensor nodes that responsible for processing and transmission of data towards a central location.

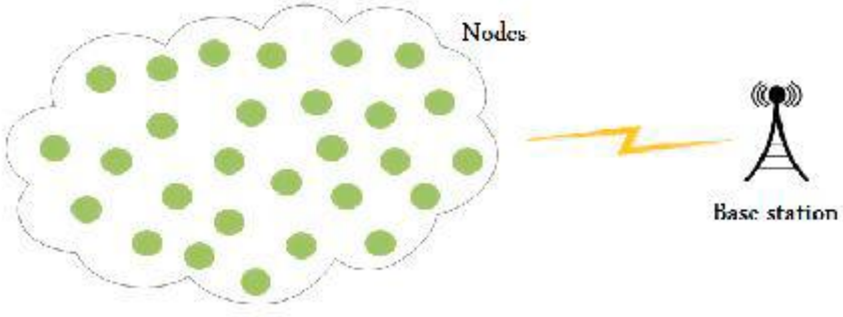


Fig.1.A wireless sensor network's basic architecture

The network becomes unreliable in terms of operation and communication when it has been affected due to various attacks. It's required to focus on dealing with different attacks of a network layer, such as acknowledgement flooding, false routing, hello flood, selective forwarding, wormhole, and sink hole [10-11]. One of the severe security attacks of WSNs is the black hole attack, which could be detected based on Hidden Markov Model method [12].

Possible Attacks on LEACH

Preventing the accurate and entire sensing data at the Base Station that could be severe for WSNs is the attacks. The sinkhole attacks have been restricted for a definite level using many secure routing methods based on topography. The sensing data continuously forward to the BS or sink node based on a tracking of neighboring nodes by the group of sensor nodes.

LEACH protocol has been included different attacks that minimize the overall network performance. The major attacks of LEACH are included as follows [13]:

Sybil Attack:

In the peer-to-peer network types, these attacks are counted majorly. The malicious node tracks the genuine node's identity in this attack. In case of communication, two nodes are involved in the process while the malicious node has been captured the communication and tried to disclose other nodes as legitimate for information exchanging. In such way, all data can be taken by an opponent.

Selective Forwarding Attack:

It can be occurred at the network layer and is called as the Gray Hole attacks. This attack includes the dropping of data by a malicious node and some data share to the destination. It causes data loss that degrades QoS of WSNs. This attack is difficult to be detected and restricted [14]. Karlof and Wagner [16] were introduced these attacks, where the data packets forwarding is refused or dropped by the compromised nodes towards other remaining nodes of a network.

HELLO Flood Attack:

The hello messages sharing for other remaining nodes is considered in various protocols to be taking part of the communication. It leads to the increasing of power consumption for receiving these messages as they have higher signal strength. The main intention of an attacker node is to increase a network traffic that results in the collision [15].

II. LITERATURE SURVEY

Based on energy consumption, WSNs have two different categories like homogeneous and heterogeneous WSNs. Different energy levels could be assigned to different nodes for heterogeneous networks while the same energy is given for all sensor nodes in the network. Two different modes of operations like proactive and reactive are involved in the WSNs. In proactive networks, the periodical data transmission is occurred while reactive networks involve an immediate response. Several works have been investigated the clustering concept of WSNs [17].

Liu et al., [18] were proposed a routing method, which considers active detection of attacks and active trust. It features security, routing, and higher scalability. In this work, the active system is presented to detect the network's malicious node and not making available for a complete routing. As this routing method concerns about fewer energy to generate different routes, it consumes less energy and provides improved routing efficiency. A scalable and safe method is presented that preserving the data packets from attacks based on a two-stage security mechanism and dual assurance technique. The active trust is a relied aspect of these both techniques, in which nodes and data protection is possible against different attacks like selective forwarding and blackhole attacks.

Alaimi et al., [19] were presented a detection method for detection and monitoring of different attacks of WSNs like selective forwarding and considered to improve different methods for network monitoring. Without having much efforts, the defined method is able to identify the security attacks for a network layer. The compromised node has been operated like some other node of a system in the defined type of attack and some private data can be dropped using the malicious node in prior to the data sharing to the destination node. Two-stage security mechanisms and the dual assurance methods have been considered for a proposed method.

Mezrag et al., [20] were improved a stable and trusted routing method that utilized a dual assurance mechanism and a two-stage authentication method for choosing a node and protecting the data packets in the WSNs. During routing process, many attacks are secured using the techniques based on Active Trust. These attacks are selective forwarding and blackhole attacks. This work has an objective of designing a trustable secure routing method that includes a data routing and an active detection routing protocols to decrease the possibility for selection of attacked or malicious nodes as shared nodes.

HananeKalkha et al., [21] were proposed a Hidden Markov Model for detection of malicious nodes in WSNs based on the black hole attack prevention. The shortest path is analyzed using this proposed method based on a new routing method for restricting the path of malicious node. The simulation results were proved the efficiency and success of a proposed routing method.

III. PROPOSED SYSTEM

It's required to distribute the keys among nodes effectively. Every node is given with the key distribution and verification process. For revoking the keys of malicious nodes, the certificate revocation process is also introduced. The remaining nodes can't be contacted by the malicious nodes without any valid keys.

A Secure Cluster level Revocation Scheme

The node identity is enhanced using a symmetric cryptography technique, and a revocation process based on certificate cancellation and secure communication method that identify the safe transmission of messages with validity documentation. Here, the encryption and decryption of certificates has been occurred.

3.1 Overview of System

The Intrusion Detection System – Secure Cluster level Revocation Technique or IDS-SCRT has been introduced for WSNs. The reliability of entire messages has been validated through the broadcasting and checking of request process based on keys by sensor nodes. The nodes are formed as different clusters and the CH should be chosen according to the nodes' distance. The nodes will be chosen when they have minimum distance from a cluster for selecting as CHs. All data from cluster members is collected by the CH and group them as clusters. The related-CH could transmit the trusted messages only based on the cluster's members. Thus, the trustworthiness of entire messages are validated.

The certificate authority (CA) is considered as the trusted third party that could be responsible to revoke and distribute the certificates related to the mobile nodes. The certificates with in-detail information broadcast to the intermediate nodes using the CA and it is called as hop. Then, the broadcasted information transmits to each CH that locates within the scope. The nodes can be attacked by the transmission of fake certificates or keys. The validity of a certificate is included in the attacked node although it may lose its certificate. From a cluster, the revoked nodes are chosen based on a criteria while this node preserves in the certificate revocation list or CRL. At the CA, the information about CRL maintains and accumulates the identities of revoked nodes in addition to the conversion into a single value based on an accumulator, known as universal accumulator. In prior to the expiration dates of certificates, the attacked nodes revoke with them using a CA. As a result, the witness of non-membership is validated by the accumulator for witness nodes that ensures the validity period of a certificate as not over-ridden. When a certificate gets the relevant non-membership witness, its legitimacy is validated by the network's entity based on this accumulated measure. Instead of transmitting the valid certificate data to the nodes of a cluster, it issues to the CH using a CA.

It could request the CH in case of requiring the certificate data by any of the cluster members. Based on a symmetric cryptography method, the messages' transmission is occurred securely when a CH detects the valid certificate after receiving the details. In this method, the certificates with decryption and encryption may occur. The proposed method is showed in the Figure 5.

Trusted Authority (TA): In the case of any misconduct, the confidential third party, known as TA is generated the secret key, principal public key, structure factors, and secret key of participants, and mobiles nodes' tracing from virtual characteristics, and preloading them to mobile nodes.

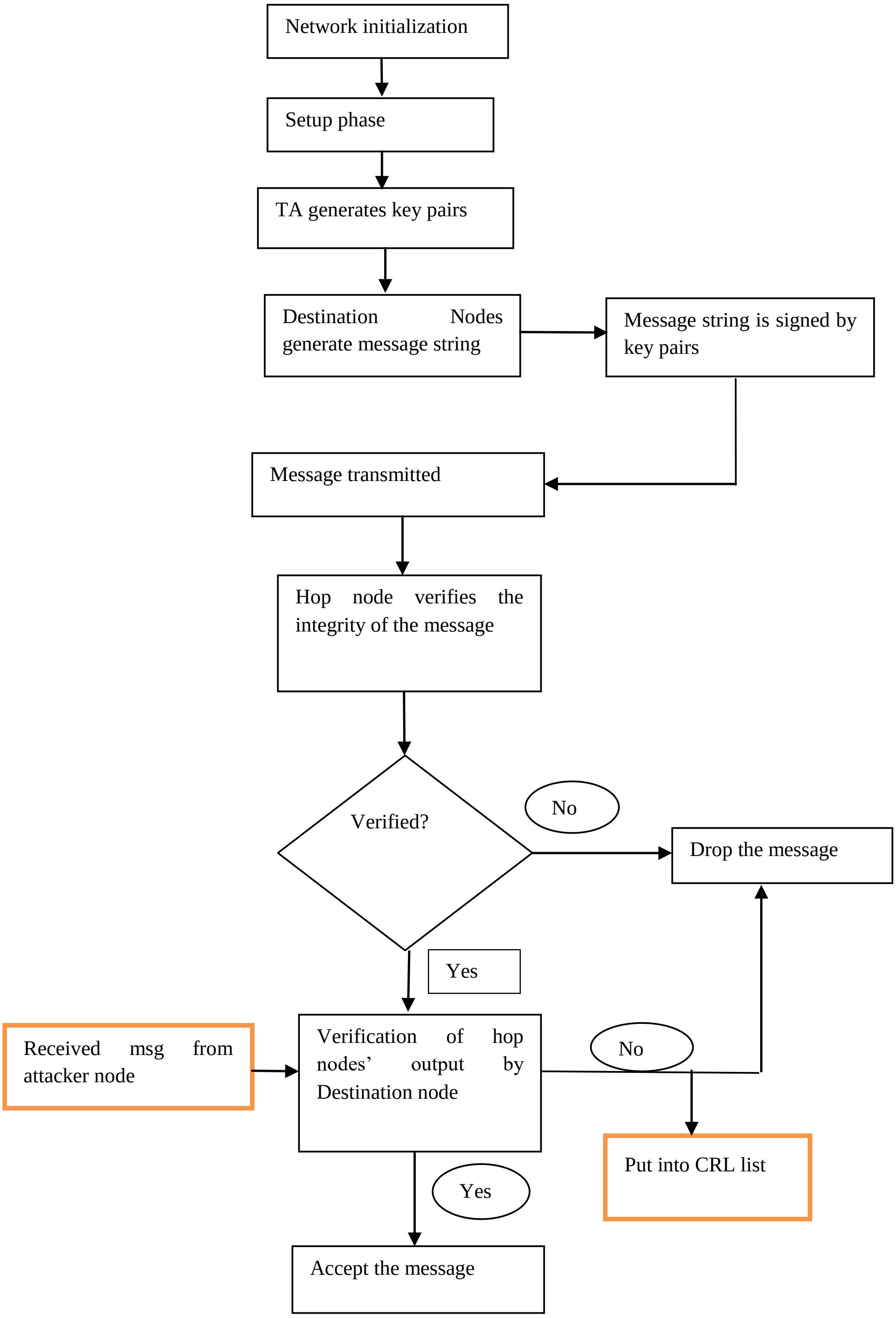
In this scheme, four phases are involved, such as:

i. **Certificate Authority:** This phase is responsible to distribute and revoke the certificates that related to the nodes. The TA recognized as hop node when transmitting the certificates' particulars towards the intermediate nodes. Within a range of nodes, the broadcasted details receive by each neighbor node.

ii. **Message generation:** In this phase, a timestamp t transmits the selected message by each node towards the hop node.

iii. **Messages verification by hop node:** This phase has a validation of sender's identity for received messages using a hop node. The complete network process' participants transmit the trusted messages using a related-neighbor node. The whole messages' trustworthiness has been verified.

iv. **Output of hop nodes verification by destination node:** Based on the obtained results from hop nodes, the revoke mischievous hop nodes and false outcomes have been identified and a destination node is verified. To perverse the revoked node in CRL, this node is chosen from a network area while following the principles. The nodes' certificates are considered as malicious nodes that would be added into the CRL.


Network initialization
Setup phase
TA generates key pairs
Destination Nodes generate message string
Message string is signed by key pairs
Message transmitted
Hop node verifies the integrity of the message
Verified?
No
Drop the message
Yes
Received msg from attacker node
Verification of hop nodes' output by Destination node
No
Put into CRL list
Yes
Accept the message

IV. RESULT AND DISCUSSION

4.1 Experimental Setup

The proposed method's performance is analyzed based on simulation results with the comparison of two different methods. The NS2 simulator is used in this work and it is a discrete event-driven and object oriented network simulator. The simulation of multicast protocol, routing, and UDP is provided for all wireless networks. The network model has been utilized in this work, where all sensor nodes are fixed, uniformly deployed, featuring homogeneous, and have included similar initial energy. In a network, the base station location is fixed and distant away from a sensor node. Based on static nodes and plane coordinates, simulation tests are performed. Here, the nodes are transmitting or receiving data after using the nodes' initial energy while they assume as having limited energy supply. As shown in Table 1, the simulation parameters are given. The proposed method is studied using a network simulator (NS2) version of 2.35. In the simulation, the network consists of 25 sensor nodes over the area of 800m*541m. However, the mobility of random way point (RWP) is used and set the transmission range to 250m for ideal amorphous. The 'code.tcl' is used to create the traffic randomly with the use of two scripts for constant bit rate (CBR) of 1000 bytes based on UDP protocol. All tests are conducted by considering the simulation time as 10 sec.

PARAMETER	**VALUE**
Traffic Protocol	CBR
Packet rate	1000 bytes/ 0.1ms
Communication range	250m
Packet length	1000 bytes
Routing Protocol	AODV
Total time of Simulation	100sec
Number of nodes	25
Area of network	800 x541
Malicious nodes	1
Transmission Protocol	UDP
Initial Energy	100j
Routing methods	IDS-SCRT, HMM, ISFC-BLS

Table1: Simulation table

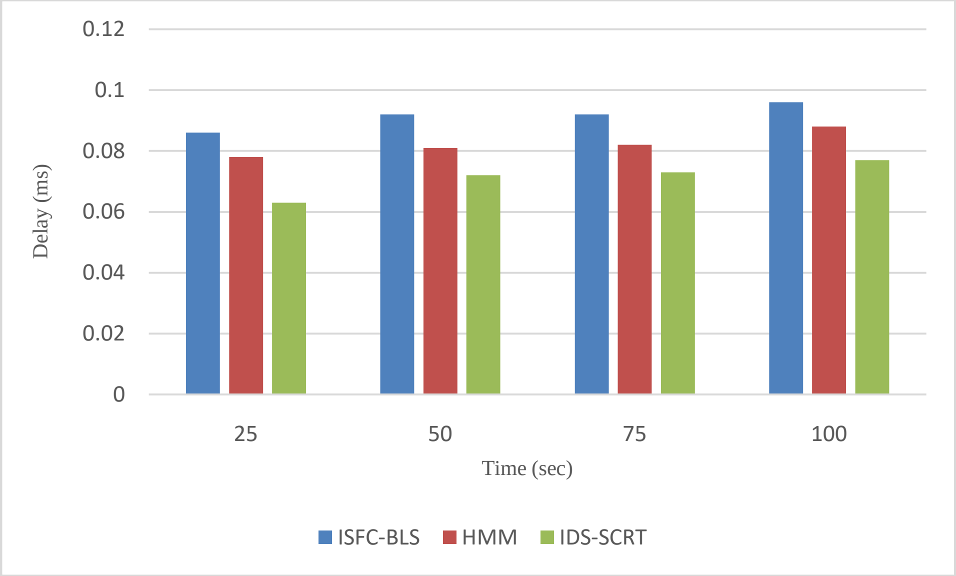


Fig4: Performance on Delay

Figure 4 shows the delay performance results for proposed and existing methods. The delay of data delivery is higher when proper forwarder nodes are not chosen. The node forwarding behavior is viewed by the monitoring agent of a node and the nodes that have poor delivery rate will be avoided. This will affect the network delay and less end-to-end delay is provided for a proposed method in comparison with other existing techniques.

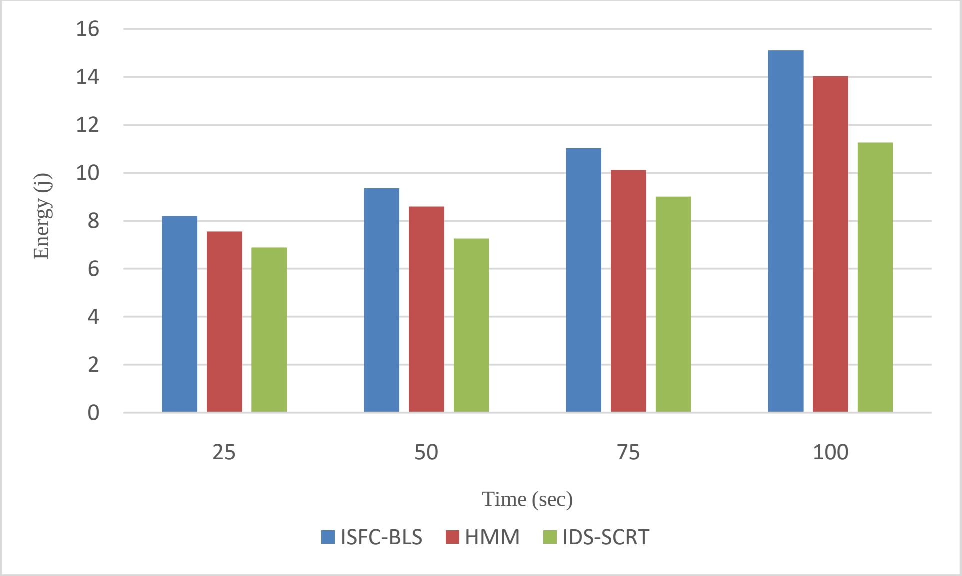


Fig5: Energy Consumption

Figure 5 illustrates the simulation results of energy consumption for IDS-SCRT method and earlier techniques like HMM and ISFC-BLS. Energy consumption is the major factor for causing a network failure due to the limited source of WSNS. The data forwarding among nodes is ensured with the optimized energy usage by using a secure certificate revocation process. The proposed approach shows improved power consumption and enhanced network lifetime than the other protocols.

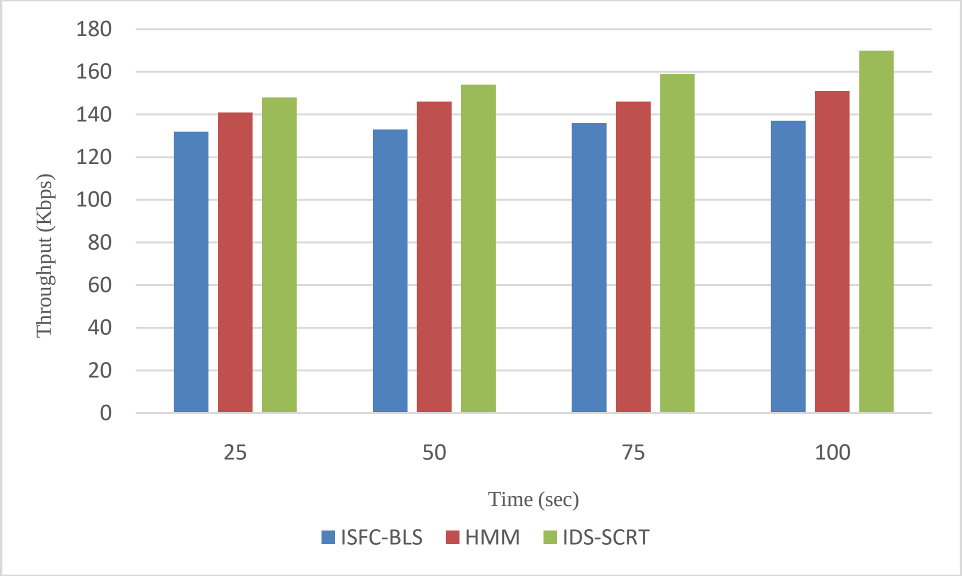


Fig6: Network Performance

Figure 6 displays the network performance or throughput of proposed technique and previous methods like HMM and ISFC-BLS. Throughput is defined as the successful data packets transmission to process reliable communication. The effective data delivery is provided with the forwarder nodes' fair selection based on past activities that impacts the network throughput highly. The improved throughput is provided using a proposed method than the other methods.

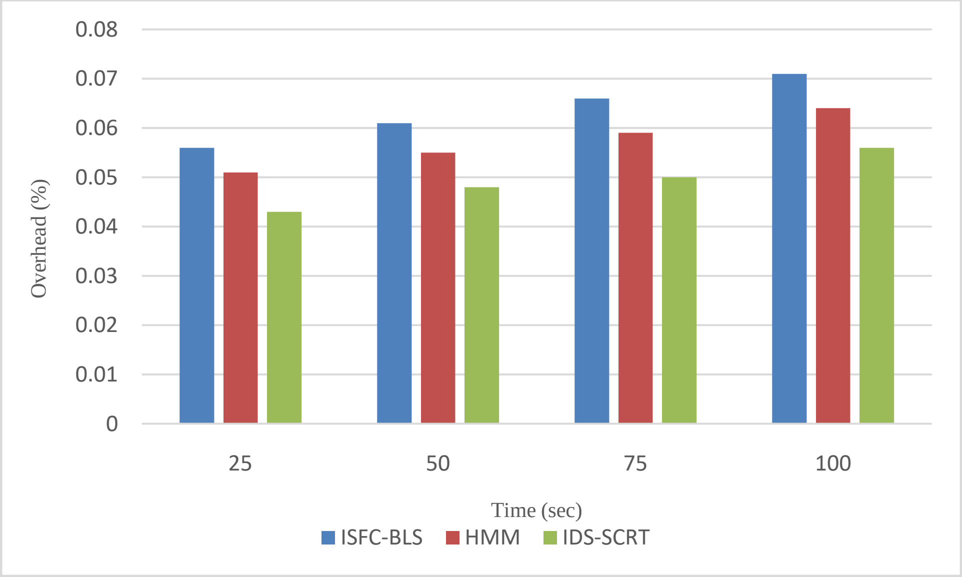


Fig7: Routing Overhead

Figure 7 shows the routing overhead simulation graphs for a proposed algorithm. The network security is achieved using a revocation process. The proposed method is achieved the lower overhead compared to other previously used methods.

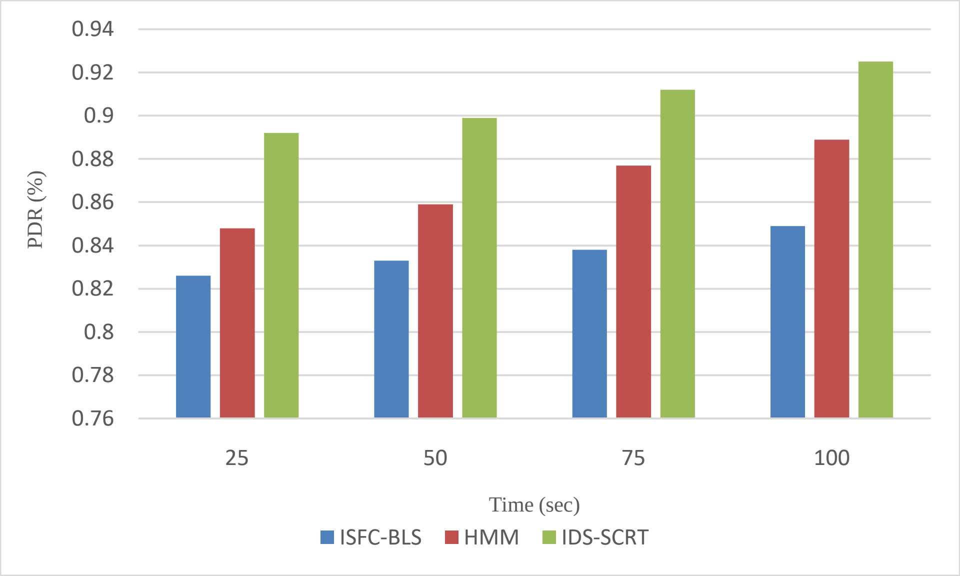


Fig8: Packet Delivery Ratio

Figure 8 describes the packet delivery ratio results for proposed IDS-SCRT method, which outperforms in processing the transmissions effectively. The seamless data delivery improves within the estimated data and the data will deliver quickly. The proposed technique shows better performance in terms of higher PDR rate by comparing with other protocols.

Conclusion:

A new intrusion detection system based cluster level certificate revocation method (IDS-SCRT) method is proposed for enforcing the wireless sensor networks' security. The generated nodes are used over a network for effective distribution of keys among sensor nodes. The hop nodes are given with the key distribution and verification process. For revoking the keys of malicious nodes, a certificate revocation process is also implemented. Further, the contacting of malicious nodes to the remaining nodes is performed without valid keys. The simulation results are showed that the proposed method achieves efficient results in terms of throughput, packet delivery ratio, end-to-end delay, energy consumption, and routing overhead by comparing with other existing techniques.

REFERENCES

[1]. Rajeswari, Kasilingam, and SubbuNeduncheliyan. "Genetic algorithm based fault tolerant clustering in wireless sensor network." *Iet Communications* 11, no. 12 (2017): 1927-1932.

[2]. Gaglio, Salvatore, Giuseppe Lo Re, Gloria Martorella, and Daniele Peri. "WSN Design and Verification Using On-Board Executable Specifications." *IEEE Transactions on Industrial Informatics* 15, no. 2 (2018): 710-718.

[3]. Jayatunga, E.H., Ranaweera, P.S. and Balapuwaduge, I.A.M., 2021. Blockchain advances and security practices in WSN, CRN, SDN, opportunistic mobile networks, delay tolerant networks. In *Revolutionary Applications of Blockchain-Enabled Privacy and Access Control* (pp. 1-34). IGI Global.

[4]. Rashmi, S., Shankaraiah, N., Pooja, H.K., Goutham, B. and Upanya, M., 2021. Performance Evaluation of Wsn to Monitor Safety Parameters of Ac Transmission Line. *Wireless Personal Communications*, *121*(3), pp.1805-1820.

[5]. Lin, H., Weng, B., Pan, J., Lin, C. and Yang, Q., 2021, July. Application of Wireless Sensor Networks in the Sensitive Data Security of Intelligent Data Center under the Big Data Environment. In *Journal of Physics: Conference Series* (Vol. 1982, No. 1, p. 012017). IOP Publishing.

[6]. Singh, R., Awasthi, L.K. and Sharma, K.P., 2021. Distributed denial-of-service attacks and mitigation in wireless sensor networks. *Distributed Denial of Service Attacks: Concepts, Mathematical and Cryptographic Solutions*, *6*, p.67.

[7]. Minnoor, N., Shree, B.P. and Sahana, B., 2021, December. Evaluation of Security Aspects of Wireless Sensor Networks. In *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.

[8]. Sharma, A.S. and Kim, D.S., 2021. Energy efficient multipath ant colony based routing algorithm for mobile ad hoc networks. *Ad Hoc Networks*, *113*, p.102396.

[9]. Lazrag, H., Chehri, A., Saadane, R. and Rahmani, M.D., 2021. Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, *33*(22), p.e6144.

[10]. Abdollah, Kavous-Fard, Wencong Su, and Tao Jin. "A Machine Learning Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids." *IEEE Transactions on Industrial Informatics* (2020).

[11]. Gurung, Shashi, and Siddhartha Chauhan. "A novel approach for mitigating route request flooding attack in MANET." *Wireless Networks* 24, no. 8 (2018): 2899-2914.

[12]. Mehetre, Deepak C., S. EmaldaRoslin, and Sanjeev J. Wagh. "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust." *Cluster Computing* 22, no. 1 (2019): 1313-1328.

[13]. Perrig, A., Szewczyk, R., Wen, W., Culler, D., &Tygar, J. (2002). SPINS: Security protocols for sensor networks. Wireless Networks Journal, 8(5), 521–534

[14]. Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., &Kruus, P. (2004). Tinypk: Securing sensor networks with public key technology. In Proceedings second ACM workshop security of ad hoc and sensor networks (SASN ’04) (pp. 59–64).

[15]. Liu, A., &Ning, P. (2008). Tinyecc: A confgurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings seventh international conference information processing in sensor networks (IPSN ’08) (pp. 245–256).

[16]. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures in Ad Hoc. Networks, 1(2), 293–315.

[17]. Santos, Andréa Cynthia, Christophe Duhamel, and Lorena Silva Belisário. "Heuristics for designing multi-sink clustered WSN topologies." *Engineering Applications of Artificial Intelligence* 50 (2016): 20-31.

[18]. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). Active trust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013–2027.

[19]. Alajmi, N. M., &Elleithy, K. (2016). A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks. In Proceedings in 2016 IEEE long island systems, applications and technology conference (LISAT), Farmingdale, NY, USA (pp. 1–6).

[20]. Mezrag, F., Salim, B., &Mellouk, A. (2017). Secure routing in cluster-based wireless sensor networks. In GLOBECOM 2017–2017 IEEE global communications conference. IEEE.

[21]. HananeKalkha, Hassan Satori, Khalid Satori, Preventing Black Hole Attack in Wireless Sensor Network Using HMM, Precedia Computer Science, Volume 148, 2019, Pages 552-561. https://doi.org/10.1016/j.procs.2019.01.028.