TWO-TIER SECURITY MECHANISM FOR MALIGNANT DETECTION IN WIRELESS SENSOR NETWORKS

[1] Dr.K.Gunasekaran, [2]Dr. Ashok kumar,[4]Dr. M.N.Saravana Kumar , [4]R.Swetha

[1]Professor, Siddartha Institute of Science and Technology
[2]Assistant Professor, GRT Institute of Engineering and Technology
[3]Assistant Professor, Erode Sengunthar Engineering College
[4]Assistant Professor, Sri Venkateswara College of Engineering and Technology

Abstract
Two-tier Security Model for Node Verification is proposed to provide strong security during network communication. This improves the safeguard measures in regards of privacy of sensed information as well as provides authentic communication. Nodes present in the system needs to be communicated in a secured manner; and therefore two level securities are carried out in this proposed scheme. Level 1 includes selection of trustable nodes that includes elimination of malicious node from the communication process by computing node trust ratio. Level 2 includes key generation process for the selected trustable nodes using asymmetric random key generator and removes the illegitimacy nodes completely from communication process. Two-tier Security Model for Node Verification scheme have huge capability in detecting malignant nodes by providing two level securities also tolerates numerous security attacks. Simulation results are shown and proved that projected mechanism has good output with better delivery rates and key matching ratio.

Keywords: *Trust computation, Hub Contact Rate, Random key generator, Node Authenticity, Sign verification.*

I Introduction

In the latest years, wirelessly sensor nodes are most widely used for sensing and delivering the infrastructural report. Sensor nodes that are fixed over the network to observe the circumstances and update the information to the controller either with single hop operation or multi-hop operation. Maintaining network safety is a difficult task since antagonist can effortlessly add fake info in the system for distracting the atmosphere.

The process of verifying node identity is termed to be node authentication which is carried out in order to guarantee that the data is originated from the authenticated node or source. Data confidentiality, integrity and authenticity all these three metrics is essential for proving the node authenticity and to achieve better system performance. ActiveTrust [1] was highly preferred for excluding black hole attacks. Here a number of detection routes were created for obtaining the nodal trust value quickly and thus in-turn improves the data route security. Identifying malicious hubs is significant in order to avoid eavesdropping of data. Therefore one of the security schemes named Binomial Principle System (BPS) technique is utilized [2] for offering security. Fake path is produced by using BPS here source, sink and

routing hubs does not reveal their real node ID's and information ID's in order to protect the data from the malicious observer.

II Related Work

Lots of authentication based security schemes were proposed and few protocols were discussed here for the reference. Classification of attacks in WSNs on basis of protocol stack layers is discussed in [3]. As a security measurement attack detection methods were also explained along with the eleven typical attacks. Data Aggregation (DA) combined with a security mechanism can provide better solution and to ensure the security of a WSN without decreasing its network performance [4]. Review analysis of Secure DA (S_DA) in WSNs, was discussed along with their security goals in terms of application scenarios. An efficient scheme named Authentication and Key Establishment (AKE) [5] was proposed for dynamic sensor network. Every sensor nodes in network maintains a table referred as 'key cache' for managing the keys generated and it is verified by pairing with the BS key. For high security level mobile sensor nodes also gets authenticated with new neighbouring nodes by pairing the keys.

Secret key based user confirmation control scheme with encryption process was proposed in [6]. The client must have the best possible key with coordinating set of characteristics to recover the data from the organization. Security analysis is carried out by utilizing safe hash function of deterministic calculation. Lightweight user verification scheme for WSNs [7] utilizes responded validation and meeting key congruity. This strategy was demonstrated to show mystery, veracity, common validation and meeting key age. A security joint effort model named Security Cooperation Collection Tree Protocol (SCCTP) plot [8] was suggested that keeps a confided in climate and segregates acting mischievously hubs. This technique including coupled state vectors related with geography control and time synchronization. The organizations accomplish synchronization utilizing loads and by controlling the quantity of objectives. The basic computation of time synchronization esteems between neighbouring nodes fills and for making a decision about the conduct of the node geography control.

Hybrid Secure Data Transmission Scheme (HSDTS) [9] for WSN was proposed. Here hybrid security scheme is applied by verifying the node's originality using reputation values by applying grade factor calculation method initially. Then improved SHA based security algorithm is added for data encryption and decryption to provide strong security network. Secure key age with lightweight encryption [10] system was proposed here the sensor hubs are set in a made sure about area.

Two way confirmations are applied for made sure about correspondence between hubs. Confirmed Anonymous Secure Routing (CASR) conspire [11] used to ensure fiery assaults. Mystery check message is made utilizing the key-encoded onion routing function. Specification of high secrecy and security seems to be a favourable position. However, there is tremendous delay during information transmission. Sensor outcome reports are utilized to discover the malignant hubs and estimate their severity of attack.

The acknowledgment cycle is inspected utilizing the entropy-unmistakable trust model [12]. Physical Layered with Secure Key Generation (PL-SKG) conspire was proposed [13] to lessen the measure of key material that gadgets needed for the arrangement. The data is made sure about utilizing ECC keys and keeps it from spilling local hubs.

III Proposed work

Two-tier Security Model for Node Verification (TSMNV) is proposed to provide strong security during network communication. This two level security scheme highly improves info privacy in the entire system. Level 1 includes selection of trustable nodes that includes elimination of malicious node from the communication process by computing node trust ratio. Level 2 includes key generation process for the selected trustable nodes using asymmetric random key generator and removes the illegitimacy nodes completely from communication process.

(i) Level 1 - Selecting Trust Node

The trustable nodes in the network can be identified by computing Hub Contact Ratio (HCR). HCR is calculated by taking route request message (Rq-msg) and route reply message (Rp-msg) that sent each other for detection of hubs that present in the range of communication. On basis of the difference between the number of Rq-msg received from the particular node and the number of unsent Rp-msg's to the number of Rq-msg received. The HCR is calculated by equation 1 and 2.

$$HCR = \left(\frac{Rq - (1 - \mathrm{Rp})}{Rq} \right) * 100 \quad (1)$$

where

Rq-> Get Route Request

Rp-> Unsent Route Reply

$$Rp = Rq - Rr \quad (2)$$

where

Q ->Reply sent w.r.t Route Request

Hubs or sensing nodes usually transmit the sensed information over the range of their transmission. Nodes present in their communication or contact range are grouped together and formed as cluster. Lead node in the cluster is elected on the basis of energy level and HCR. The energy level is compared with each node and the node with the higher energy as well as NCR with greater than 85% is selected. Finally, data is transmitted from the source to sink successfully.

(ii) Level 2 – Generating Secured Key

After selecting the trustable nodes from the clusters private keys are generated for all the selected hubs. BS randomly generates a coded 4-digit number 'A_n' using secured hash keying algorithm and private key is computed for each node with respect to their ID so that the node authenticity N_{ai} is obtained. If generated key is made as public then any of the nodes present in the system can easily access the data. Therefore signature is verified by matching private key then declares the hub is legal and can be accessed by the authorised nodes.

Once the node legitimacy (N_{ai}, S_{Id}(key)) is proved then the two nodes can communicate. Random key generator computes the coded key '$M_{A,B}$(k) using Message Authentication Code (MAC) to encrypt the sensed data. Hence each message (data packets) comprises of normal authentication MAC encoding key 'K' at the end (in the header field of the data packets) and this key protects overall info from eavesdropping of malicious nodes. Figure 1 shows the flow diagram of the proposed TSMNV mechanism.

Subsequent to getting the solicitation message, the BS begins validation measure by utilizing sign confirmation framework and checks the hub for lawful access. When the testament is accommodated the real hubs, the message encoding measure completes. The message from the sender hub is encoded by utilizing hashing calculation encryption system along with utilizing basic confirmation key. Later $M_{k(A,B)}$ is transferred to the receiving node with the valid sign $\{N_{ai}, Id(K_i)\}$ at the end of the encrypted message which is given in equation 3.

$$M_{(A,B)} = E_{msg} \| \{N_{ai}, S_{Id}(key)\} \quad (3)$$

Algorithm for TSMNV

Start
Build 'N' nodes in network
Get registered to BS
→ ***Level 1 to be processed***
Compute HCR
Select Trustable nodes using E_L & HCR
Cluster formation is done
→ ***Level 2 to be processed***
Generate coded keys 'A_n'
Set node 'A' → sender and 'B' → receiver
Verify nodes with 'S_{Id}'
Do node validation $\{N_{ai}, S_{Id}(key)\}$
If coded key "$S_{Id}(key)$" gets matched
Pass secured info to receiver
End

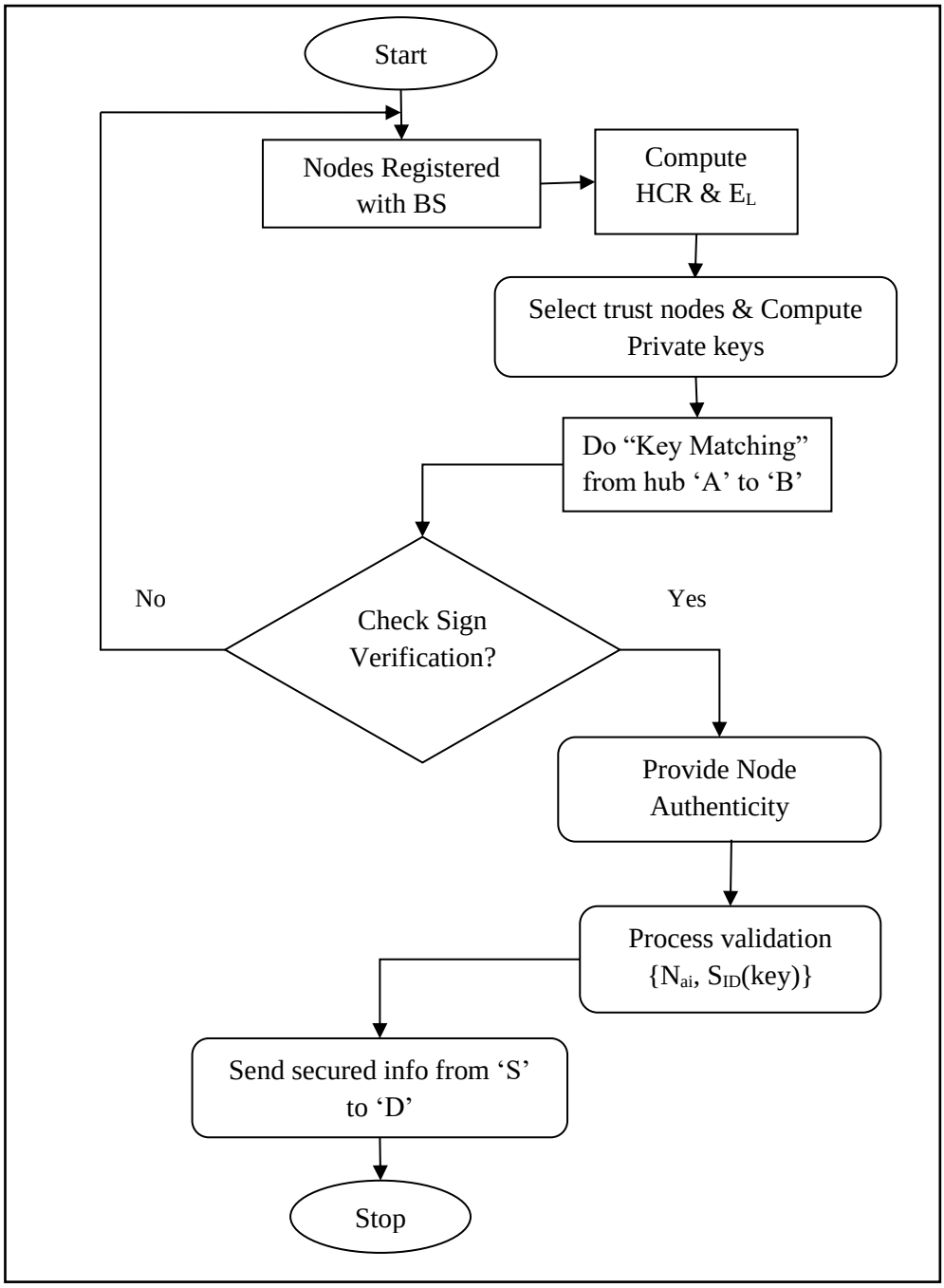

Figure 1: Flowchart of TSMNV Scheme

IV Performance Evaluation

The performance of the TSMNV system is examined with the simulation tool called Network Simulator of version-2 (NS2). 100 numbers of nodes were taken for evaluating the proposed TSMNV scheme and conventional SCCTP method. The simulating area is created with the dimensions of 1000x1500 m^2. Simulation analysis is done with the evaluation metrics such as Data Delivery Rate, Energy leftover, Delay and Matching key ratio.

Packet Rate Delivered: The pace of information packets that is successfully conveyed over the objective generated by CBR sources is called as Packet Delivered Rate (PDR). PDR measurement implies the proficiency of conveying information over the system. Equation 4 is used to calculate total number of info-packets delivered successfully; here T denotes time and n denotes node density.

$$PDR = \frac{\sum_{0}^{n} Pkts\ Delivered}{T} \quad (4)$$

Average Delay: It can be characterized as the handling time that the info packet consumes to navigate starting with one node then onto the next, and this incorporates lining delay. This measurement evaluates the achievement proportion of the TSMNV framework routing strategy. Equation 5 is used to determine packet transmission delay and ‘’n denotes for node density.

$$Delay = \frac{\sum_{0}^{n} Pkt_{\ r\,e\,cvd\,time} - Pkt_{\ sent\,time}}{n} \quad (5)$$

Mismatch-Key Ratio: Mismatch Key Ratio (MKR) is defined as the main metric to recognize false private keys generated by malicious nodes which gets mismatch when paired with BS. The ratio between various numbers of bits in the secret keys with the total number of key bits created for signature verification is said to be MKR.

Leftover Energy: An energy level that remains in the node at current instant is termed to be residual energy (energy leftover). In different terms it tends to be estimated by assessing the greatest energy devoured (consumed) by the hub and the present energy level in the hub.

Figures 2 and 3 describe the data delivery rate and leftover energy for the proposed TSMNV and conventional SCCTP schemes. The proposed scheme TSMNV has better consequences in terms of delivery rates comparing to the conventional method SCCTP.

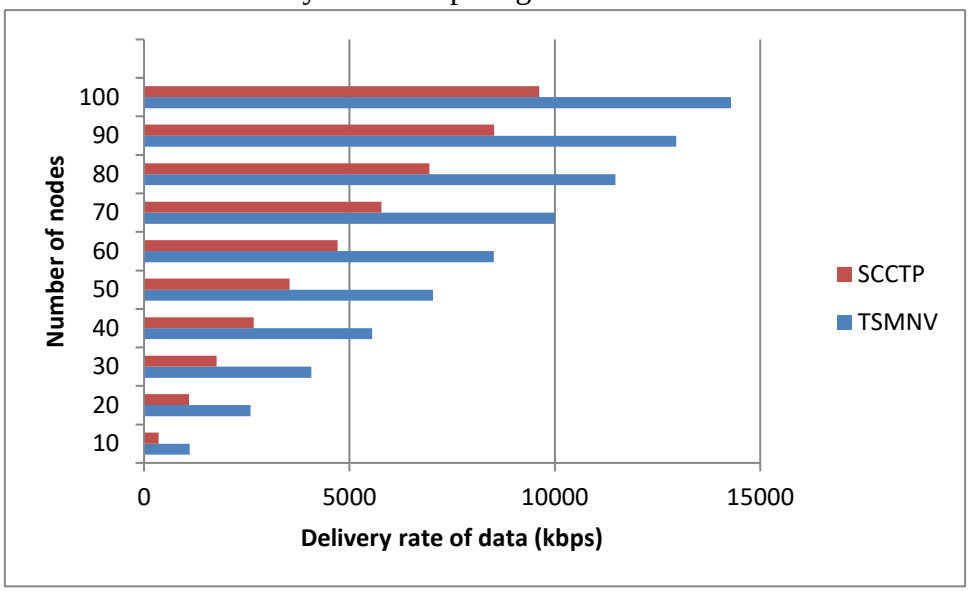

Figure 2: Data delivered rate

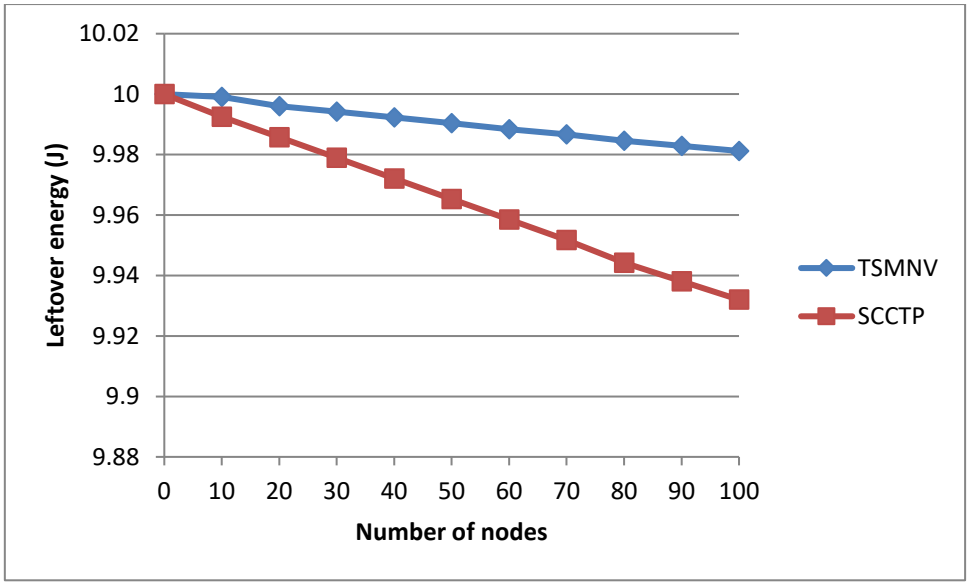

Figure 3: Leftover Energy level in nodes

Initially 10J is set for both the schemes and the energy level gets gradually reduced for each set of transmission. Leftover energy proves that the nodes in the proposed scheme TSMNV consumes less amount of energy compared to the conventional SCCTP.

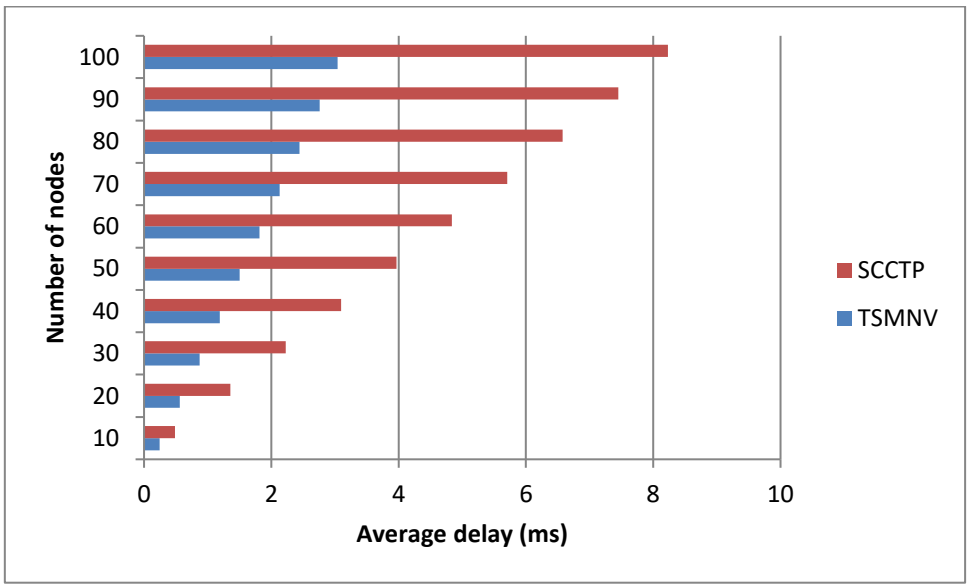

Figure 4: Delay

Average transmission delay is shown in the figure 4 for both proposed and conventional schemes. Proposed TSMNV scheme performs better in terms of packet delivery latency in comparison with existing SCCTP.

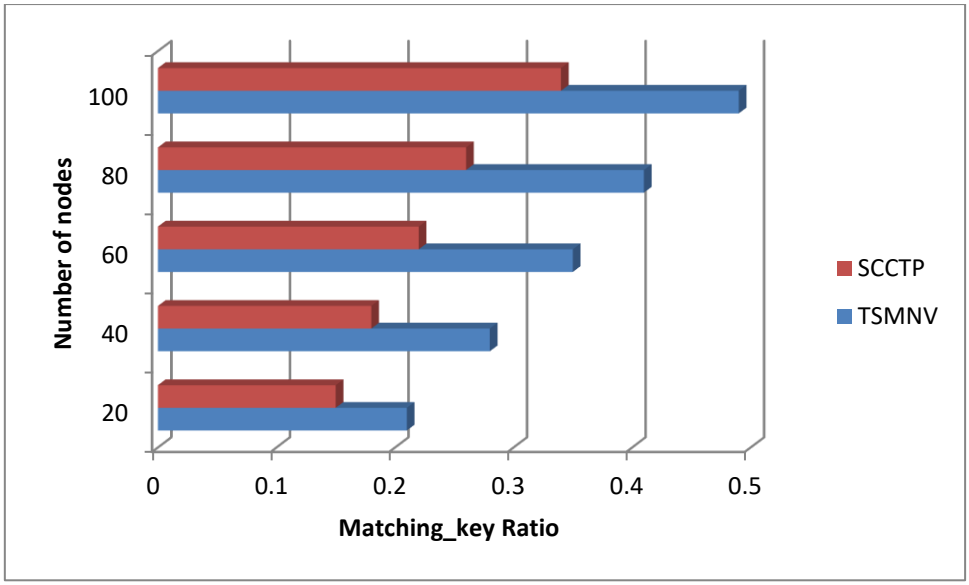

Figure 5: Matching-Key Ratio

Figure 5 describes about MKR for both the schemes TSMNV and SCCTP. It is examined and analyzed that the matching key ratio is greater for the proposed TSMNV compared to the conventional scheme SCCTP.

V Conclusion

Two-tier Security Model for Node Verification is proposed to provide strong security during network communication. TSMNV improves the level of security during the passage of information packets and ensures reliable communication. Nodes deployed in the system should have a secured communication and therefore each node in this proposed scheme is allotted with the private key. Level 1 includes selection of trustable nodes that includes elimination of malicious node from the communication process by computing node trust ratio. Level 2 includes key generation process for the selected trustable nodes using asymmetric random key generator and removes the illegitimacy nodes completely from communication process. The proposed scheme has high capability in detecting malignant node and provides good network security which can be examined through the results achieved.

References

1. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013-2027.
2. Suresh, G., & Kumar, A. S. (2020). Secure Transmission Using Bivariate Principle System for WSN. *Helix*, *10*(03), 47-51.
3. Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data collection for security measurement in wireless sensor networks: a survey. *IEEE Internet of Things Journal*, *6*(2), 2205-2224.
4. Liu, X., Yu, J., Li, F., Lv, W., Wang, Y., & Cheng, X. (2019). Data aggregation in wireless sensor networks: from the perspective of security. *IEEE Internet of Things Journal*.
5. Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," *Sensors*, vol. 10, no. 4, pp. 3718–3731, 2010.

6. Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2013). Light-weight framework for security-sensitive wireless sensor networks applications. *IET Wireless Sensor Systems*, *3*(4), 298-306.
7. Chatterjee, S., & Das, A. K. (2015). An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks*, *8*(9), 1752-1771.
8. Liu, Z., Liu, W., Ma, Q., Liu, G., Zhang, L., Fang, L., & Sheng, V. S. (2019). Security cooperation model based on topology control and time synchronization for wireless sensor networks. *Journal of Communications and Networks*, *21*(5), 469-480.
9. DAS Kumar (2020). Hybrid cryptography key based Secure Data Transmission Scheme for Wireless Sensor Network. In *Alochana Chakra Journal 9 (Issue IV, April/2020), 1120 - 1127*.
10. Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2013). Light-weight framework for security-sensitive wireless sensor networks applications. *IET Wireless Sensor Systems*, *3*(4), 298-306.
11. M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, "Distributed detection in mobile access wireless sensor networks under byzantine attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 4, pp. 950–959, 2014.
12. Shen, H., & Zhao, L. (2013). ALERT: an anonymous location-based efficient routing protocol in MANETs. *IEEE Transactions on Mobile Computing*, *12*(6), 1079-1093.
13. Moara-Nkwe, K., Shi, Q., Lee, G. M., & Eiza, M. H. (2018). A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks. *IEEE Access*, *6*, 11374-11387.