Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 3546-3553

Research Article

Swarm Intellect Optimization Technique (SIOT) based mischievous detection and improve Authentication in Mobile Wireless Sensor Network

[1]D. Joseph Jeyakumar, [2]Adam Raja Basha

[1]Professor, Department of Electronics and Communication Engineering, J.N.N Institute of Engineering, Chennai, Tamil Nadu, India, jayakumarjoseph33@gmail.com.
[2]Associate Professor, Department of Electronics and Communication Engineering, Audisankara College of Engineering and Technology, Gudur, Andhra Pradesh, India.

Abstract

Mobile Wireless Sensor Network (MWSN) typically created with no major infrastructure. Thus, they are moderately defenseless to various mischievous attacks; as a result, attack detection is a significant problem in MWSN. The cryptographic technique can avoid several attacks. A mischievous node can simply disrupt a route in the communication path. However, an attacker captures sensor nodes, evokes their cryptanalytic key, and modifies their code to behave mischievously. Hence, the mischievous node detection is a significant problem in the network. To solve these problems, in this paper, Swarm Intellect Optimization Technique based mischievous detection and improve Authentication in MWSN. In this approach, the minimum distance nodes are formed the clusters. Then cluster Heads (CHs) are selected based on the node weight. Observing forwarding behavior, Observing Great energy Communication and Observing fake route ads parameters are decided the MWSN Mischievous nodes. The presented approach is validated by a network simulator. Simulation results shows the SIOT approach detect the mischievous nodes efficiently.

Keywords: Mischievous Node Detection, Authentication, Swarm Intellect Optimization Technique, network simulator, Mobile Wireless Sensor Network.

1. Introduction

A Mobile Wireless Sensor Network (MWSN) is an essential element of the wider period and MWSN is a transitory independence system collected through a group of mobile nodes with the wireless sender-receiver set [1]. Every node has the individualities of host computer as well as the router. Rendering to, the MWSN is designated as a network which cooperate to intellect data about its domain, in addition thus adjusting the surrounding situation. Because of, the variety of its applications in healthcare, military, industrial control also observing many more, have developed as a leading technology for the forthcoming [2].

Wireless networks are susceptible to security attacks owing to the environment of the wireless transmission medium. MWSNs have extra susceptibilities because of the resource restrictions in the sensor nodes [3]. Furthermore, the sensor nodes can be arranged in an unattended situation that creates them substantially dangerous also can be apprehended through mischievous [4]. The cooperated sensors may not only be utilized for delivery of unwanted otherwise false details, but can also reduce the function of the whole network. Hence, the security of MWSNs develops a main apprehension which attracts several investigators. Several routing approaches in MWSNs are not initially intended with security deliberations because of the resource boundaries on the mobile sensor nodes. It can variety them susceptible to several kinds of attacks [5].

The nodes in MWSN is usually divided into specific clusters, some nodes known as CHs that is accountable for allocation of resource to cluster member nodes in its cluster. Clustering technique necessitates the collection of a CH applying definite important factors which designate the suitability to play as a CH. Every nominated CH is accountable for resonant topological information to continue network connectivity [14]. An innovative cross-layer authentication approach which incorporate steganography based authentication as well as physical layer authentication is introduced for massive cellular Internet of things. A cross-layer authentication approach is intended with a incorporation approach lower the disseminated authentication structure. However, this approach increases the complexity and enhances the false detection of Mischievous nodes [15].

2. Literature Review

Mobile Agent based Mobile Mischievous Node Detection is used to identifies the mobile mischievous node applying the mobile agent. In this approach, the multi-mobile agents are utilized to gather the data beginning sensor nodes following confirmation. In this approach, it can be resolved through grouping into clusters as well as a particular mobile agent executes confirmation with entire CHs rather than confirm entire sensor nodes [6]. Distributed recognition of mobile Mischievous node attacks plan is to concern sequential hypothesis testing to determine nodes which are silent for abnormally several time periods this nodes are probable to be acting as well as block them from transmitting. It hold lesser energy utilization and lesser routing overhead. However, it increases the packet drop rate in the network [7].

An adaptive distributed system is an intrusion detection system is established on distributed techniques with a cooperative decision-making procedure. It is a forecasting evaluation approach for measuring the sensor behaviours [8]. dynamic network security approach represent a direct trust value that is accepted on its behavior. In this approach, the node reliability as well as nodes management is informed intermittently. Mischievous nodes are discovered with inaccessible along with the reliability to make-sure the active, protected, as well as dependable operation. Next, widespread trust value is computed by the suggestion of trust value with assessment of energy value [9].

An efficient as well as secure Mischievous node detection approach established on a hybrid clustering network by a trusted mobile node. It avoids Black hole Attack and Man-in-the-Middle Attacks [10]. Blockchain trust model (BTM) build the blockchain data structure that is applied to notice the Mischievous nodes. It comprehends the recognition of Mischievous nodes via employing the blockchain smart agreement as well as the parallelogram capacity localization approach. In addition, the voting agreement results are entered in the blockchain disseminated [11].

In this approach, Support Vector Machine learning approach is used to discover the Mischievous Node in a network. Support Vector Machine method is used for time series prediction has been applied to discover the Mischievous nodes established on the past values obtain through individual nodes [12]. Secure Data Aggregation Protocol (SDAP) that recognizes the Mischievous node through offering a logical group. Here, the aggregation is produced through an aggregating the nodes, also great level of trust is necessary to offer a better estimation with accuracy alongside the security threats. As a result, the information is steadily collective with the effectiveness is attain in collecting the data [13].

3. Proposed Method

Swarm Intellect Optimization Technique is used to detects the mischievous nodes in the MWSN. Here, the mobile sensor nodes are formed the clusters by mobile node distance. Figure 1 Example for Scenario of Cluster. In WSN, sensor nodes have restricted energy resources but the usage of clustering technique is an important to raise the energy efficiency, minimize the communication delay, and also increase the network lifespan. In this approach, the minimum distance nodes are formed the clusters. Then cluster Heads (CHs) are selected based on the node weight. Here, every node maintains the global weight value. Primarily, we expected that entire sensor nodes are reliable and these exist the highest weight value. Furthermore, the node weight value decrements slowly established on the node's misbehaviour as detected through other nodes.

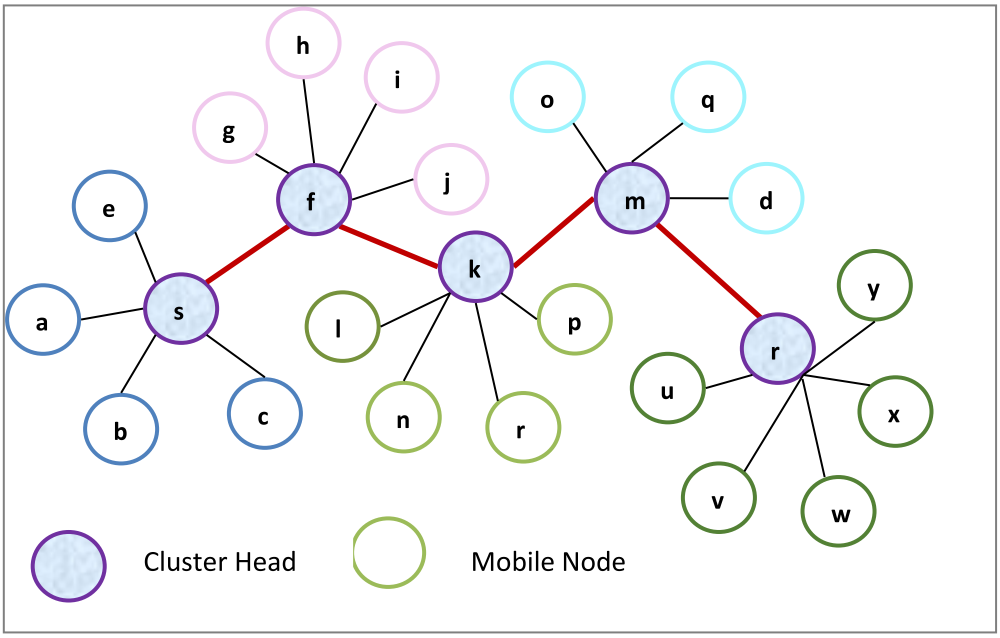

Figure 1 Example for Scenario of Cluster

Every node distinct weight values are assigned and it is not exposed through other nodes excluding the combined weight values that are mutual between the nodes. Moreover, we assumed which computation as well as collection of weight values are secure as well as healthy besides misbehaviour handling.

The highest weight factor node is selected as a CH. Every CH node nearby computes and continues a weight value for other CH nodes established on its individual experience of communication with every node. Hence, a CH node behaviour is observed also measured through all its communicating nodes.

3.1 Mischievous Nodes Detection:

In MWSN, the wireless signals are vulnerable to several interfering which can origin irregularities throughout announcement as well as data communication. To account for this misbehaving's, a misbehaviour threshold is recognised established on the references.

If a node surpasses them is behaviour threshold, next its conforming weight value is decremented. Furthermore, we comprised a self-repair property so as to permit legitimate nodes to improve from unintentional misbehaving's affected during announcement as well as data communication.

So as to evaluate the weight values for the CH nodes in which decreasing the threshold that node is chances as an unreliable node. We confirmed that the CH node is an unreliable node by greater energy communication, publicising minimum distance path from sender to the BS, as well as losing of data packets.

1) ***Observing forwarding behavior:*** When the Attacker node obtains a packets to transmit to the BS, it can loss entire packets otherwise choosing particular packets are dropped them rather than transmitting them. In this approach, the CH transmit the packets to the BS via neighboring CH nodes, it observes the transmitting behavior of the CH nodes. An observing CH node assumes an ACK message from the BS that should be transmit through the observed CH node in the packet's evaluated Time-To-Live (TTL) value. But, the attacker node does not transmit the false ACK messages. If the observed CH node obtains a valuable ACK message from the BS also in the packet's evaluated TTL value, it represents the packets are transmitted effectively as well as that the observed CH node is normal [15]. If ACK message is does not obtained, the observing CH node waits for an arbitrary amount of period next, efforts to retransmit the data packet. If the forgotten CPU time of the observing CH node surpasses the packet's TTL value then no ACK message is obtained, it specifies failure in transmitting the packets to the next hop. Thus, the node is deliberated as a attacker node.

2) ***Observing Great energy Communication:*** The attacker node tasks great energy communication so as to chosen as a CH. Consequently, the attacker node has a stable energy source. To identify this behavior, a CH node could have a degenerate energy value no extra a threshold. If the dissolute energy value of the observed CH node is more than the fixed threshold, next, the node is specified as an attacker node.

3) ***Observing fake route ads:*** The attacker node broadcast to other nodes which it has the minimum distance route to the BS. An observed CH node equates the announced distance through the observed CH node with the distance of other CH nodes to the BS. If there are another CH nodes by a minimum distance to the BS next the observed CH node, it specifies which the observed CH node is announcing a false distance to the BS. Thus, the observed CH node is specified as an attacker node.

3.2 Mobile Sensor Node Weight Estimation

In this approach, the sensor nodes global weight value is used to detect the attacker nodes. Honey Bee Algorithm is applied for form the route from sender to BS. ABC technique is activated through the observing CH node during it monitors the irregularity among the weight it allocate for one node as well as weight it allocate to the subsequent node.

The irregularity in the weight values describe our threshold weight. If a sensor node beats the preset weight threshold, next observing the CH decides the real attacker by its global weight value collected by other sensor nodes. Suppose, observed CH is not professed as attacker through several nodes, it means which the node is a normal node.

The node fitness value is computed by the ABC algorithm. This fitness function computation is given below.

$$\frac{1}{k}\sum_{j=1}^{k}(GW_j - TW)^2 \qquad (1)$$

Here, k represents the overall weight values allotted for sensor node j through other sensor nodes, GW_j describes the global weight value of j also TW indicates the threshold weight to identify the attacker node.

Simulation Examination:

In this section, the network simulator is analyzed the SIOT and SDAP approaches. The network region is a 200 × 300 m^2 and the BS is act as a owner. Here, 100 sensor nodes are distributed randomly and sensor nodes are sensing the information and communicate the information to the BS. Average true positive rate, Average true negative rate, Average Meet Speed, and routing overhead parameters are analyzed in the WSN.

Average true positive (ATP):

It is defined at the rate that the technique effectively identify the attacker while it is there. Figure 2 illustrates the average true positive rate of SIOT and SDAP approaches. We compared the average true positive rates of our proposed algorithm and existing method based on node density. From this figure 2, the density of network raises the ATP rate is a little decline. Since additional attacker nodes are being measured and verified to recognize the real true attacker.

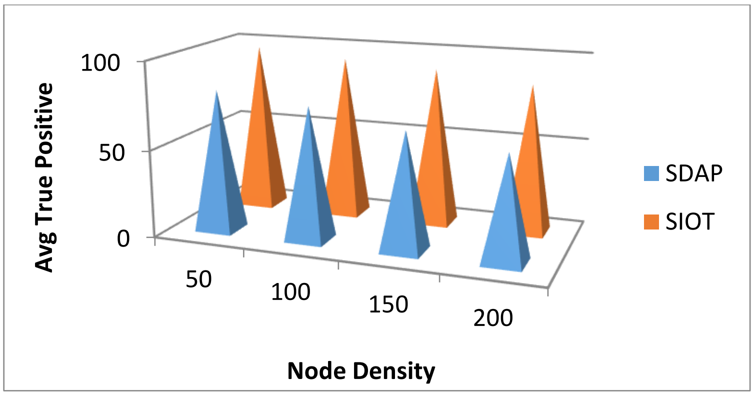

Figure 2: Average true positive rate of SIOT and SDAP approaches

Average true negative (ATN):

Figure 3 demonstrates the Average true negative rate of SIOT and SDAP approaches. ATN is defined as the rate at that the technique miscarries to identify the true attacker node. We compared the ATN rates of our proposed algorithm and existing methods based on node density. From this figure 3, the density of network raises the ATN rate is a little decline. Since additional attacker nodes are being measured and verified to recognize the real true attacker.

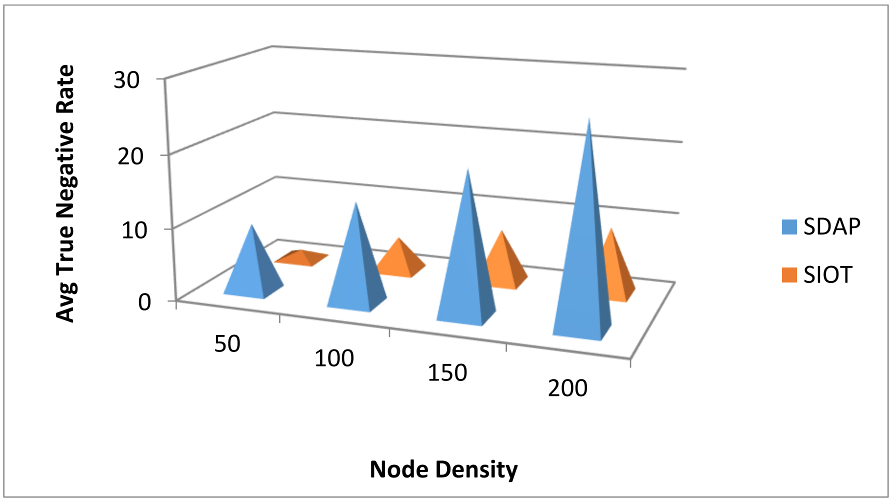

Figure 3: Average true negative rate of SIOT and SDAP approaches

Average Meet Speed: Figure 4 shows the Average Meet speed of SIOT and SDAP approaches. It represents how fast proposed techniques meets to the optimal solution, thus distinguish the real attacker node. We noticed From Figure 4, that proposed approach meet speed raises when raises the density of network. But, the proposed approach provide better attacker node reorganization accurateness and speed meet.

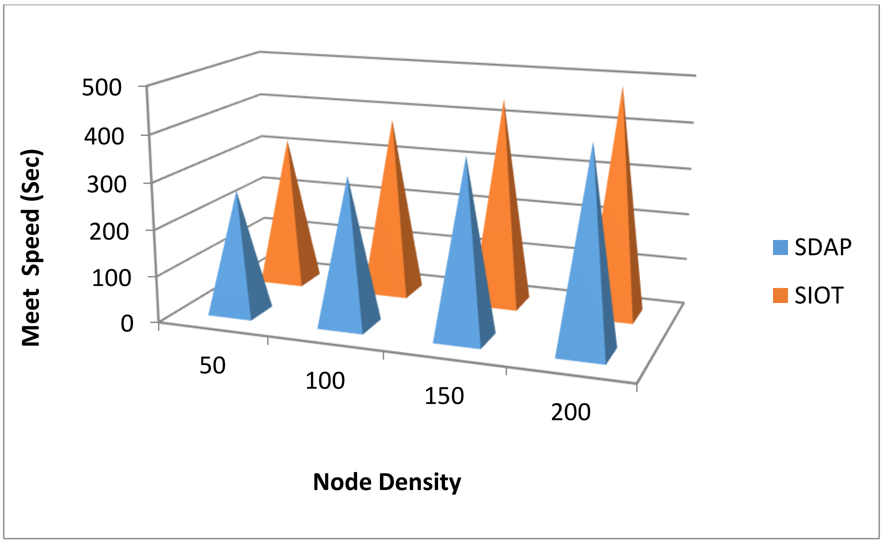

Figure 4: Average Meet speed of SIOT and SDAP approaches

Routing Overhead: Figure 5 explains the routing overhead of SIOT and SDAP approaches. Usually, noticed that the node density raises the routing overhead also increased in the network.

Because of the highest amount of nodes distributed, the sensor nodes are make additional transmission. From this figure, an SIOT approach increases the sensor node count, the routing overhead is slightly increased but, SDAP approach is highly increased the routing overhead.

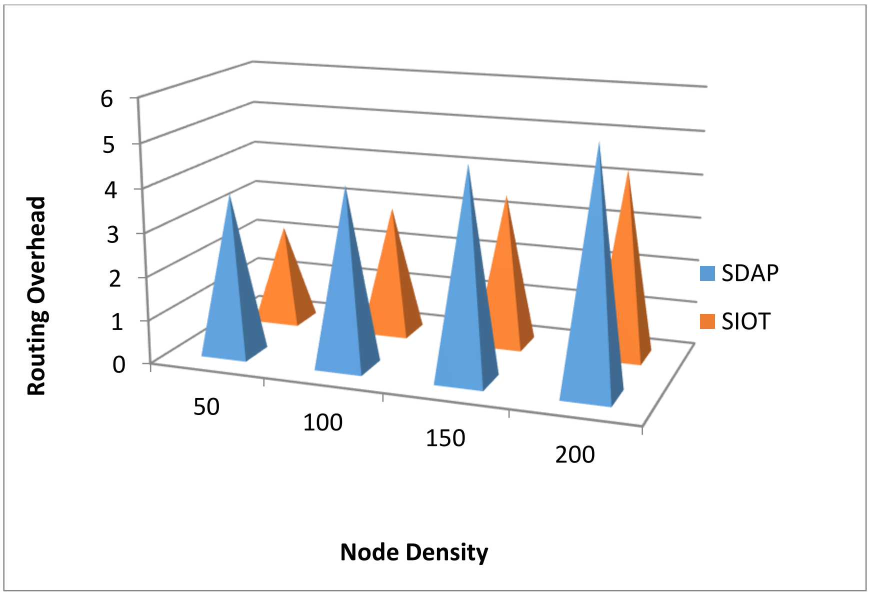

Figure 5: Average routing overhead of SIOT and SDAP approaches

4. Conclusion

This article introduced a Swarm Intellect Optimization Technique (SIOT) based mischievous detection and improve Authentication in Mobile Wireless Sensor Network. A Swarm Intellect Optimization Technique based mischievous detection and improve Authentication in MWSN. In this approach, the minimum distance nodes are formed the clusters. Then CHs are selected based on the node weight. Observing forwarding behavior, Great energy Communication and fake route ads parameters are confirmed the Mischievous nodes in the MWSN. Our simulation results explained that the SIOT approach minimizes the true negative and routing overhead. In addition, it raises the meet speed and true positive in the MWSN.

References

1. Atassi, A., Sayegh, N., Elhajj, I., Chehab, A., & Kayssi, A. (2013, March). Mischievous node detection in wireless sensor networks. In 2013 27th International Conference on Advanced Information Networking and Applications Workshops (pp. 456-461). IEEE.
2. Shahraki, A., Taherkordi, A., Haugen, Ø., & Eliassen, F. (2020). Clustering objectives in wireless sensor networks: A survey and research direction analysis. Computer Networks, 180, 107376.
3. Ahmad, M., Shah, B., Ullah, A., Moreira, F., Alfandi, O., Ali, G., & Hameed, A. (2021). Optimal clustering in wireless sensor networks for the Internet of things based on memetic algorithm: memeWSN. Wireless Communications and Mobile Computing, 2021.
4. Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486-492.
5. Olakanmi, O. O., & Dada, A. (2020). Wireless Sensor Networks (WSNs): Security and privacy issues and solutions. In Wireless Mesh Networks-Security, Architectures and Protocols. IntechOpen.
6. Gandhimathi, L., & Murugaboopathi, G. (2021). Mobile Mischievous Node Detection Using Mobile Agent in Cluster-Based Wireless Sensor Networks. Wireless Personal Communications, 117(2), 1209-1222.

7. Ho, J. W., Wright, M., & Das, S. K. (2012). Distributed detection of mobile Mischievous node attacks in wireless sensor networks. Ad Hoc Networks, 10(3), 512-523.
8. Grgic, K., Zagar, D., & Krizanovic Cik, V. (2016). System for Mischievous node detection in IPv6-based wireless sensor networks. Journal of Sensors, 2016.
9. Zheng, G., Gong, B., & Zhang, Y. (2021). Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks. Wireless Communications and Mobile Computing, 2021.
10. Morsi, A. M., Barakat, T. M., & Nashaat, A. A. (2020). An Efficient and Secure Mischievous Node Detection Model for Wireless Sensor Networks. International Journal of Computer Networks & Communications (IJCNC) Vol, 12.
11. She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for Mischievous node detection in wireless sensor networks. IEEE Access, 7, 38947-38956.
12. Jaint, B., Indu, S., Pandey, N., & Pahwa, K. (2019, October). Mischievous Node Detection in Wireless Sensor Networks Using Support Vector Machine. In 2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE) (pp. 247-252). IEEE.
13. Gomathi, S., & Krishnan, C. G. (2020). Mischievous node detection in wireless sensor networks using an efficient secure data aggregation protocol. Wireless Personal Communications, 113(4), 1775-1790.
14. Kim, B., & Song, J. (2019). Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-16.
15. Ishaq, Z., Park, S., & Yoo, Y. (2015, July). A security framework for Cluster-based Wireless Sensor Networks against the selfishness problem. In 2015 Seventh International Conference on Ubiquitous and Future Networks (pp. 7-12). IEEE.