Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1675–1680

PACKET SCHEDULING ALGORITHM VIA THE SINK NODES FOR THE ENERGY EFFICIENT MULTITARGET TRACKING IN WSNS

Bukey Chetan Manikrao[1], Dr. Vijayalaxmi Biradar[2], Dr. Sagar B. Shinde[3]

[1]Research Scholar, Kalinga University, Raipur (CG)
[2]Research Guide, Kalinga University, Raipur (CG)
[3]Research Co Guide, PCETs - NMVPMs Nutan Maharashtra Institute of Engineering and Technology, Pune

DOI
10.29121/shodhkosh.v5.i6.2024.2493

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Multitarget tracking is important research problem in WSNs since last decade. Recently improved solutions have been proposed for the same. However, some research problems that yet to address. Targets with varied importance levels invade the monitoring area, making threat assessment challenging. Some critical monitoring locations may miss high-level targets. Tracking delay reduction, energy consumption reduction, and overall network performances enhancement still needs to be enhanced.

Keywords: Packet Scheduling, Algorithm, LWKMTT Model, WSNS, Multitarget

1. INTRODUCTION

The target sensing application field may be significantly expanded because of the new technologies available in 6G, which enable ultralow latency for the transport of enormous amounts of data. Mobile target sensing in Wireless Sensor Networks (WSNs), which is dedicated to monitoring the supervisory field in the military and civilian sectors for security, is a form of a special application for the Internet of Things (IoT). Mobile target sensing in WSNs monitors the supervisory field in both the military and civilian areas to maintain safety. “This technology has several potential uses in the military, including the fight against terrorism, the navigation of unmanned aerial vehicles (UAVs), and space exploration, among other things. This application was also used to monitor no-flying zones around airports and collect information. It was utilized to provide security and acquire data. Specifically, the sensor nodes establish a communication link with the sink node and determine whether or not the suspicious target intrudes into the ground for target sensing. It is necessary to supply control data to schedule prospective sensors to carry out sensing tasks on the sink node. As a consequence of this, the sink node is considered to be a controller since it possesses enough amount of computational power for the sensor nodes.

On the other hand, because of the high latency response of the typical centralized design, optimum sensing time delinquency is becoming more and more widespread. To be more specific, the amount of time needed for computing is enhanced when enormous amounts of data are required from sensor nodes in WSNs. There is a possibility that future 6G technologies, such as terahertz channels, may be able to offer enough bandwidth for the transmission of vast amounts of data, but the unstable and short transmission connection will place additional limits on the topology control of the sensor network. In addition, duplicate data have formed as a result of the fact that many sensor nodes can identify the same target, even though target nodes are constantly moving and the coverage regions of sensor nodes may overlap in the real-world situation. Besides, transmission congestion and data queues still occur in the MTT-WSNs. As a direct result of this, the sensing time slips backward, causing the most advantageous sensing opportunity to be missed. In addition, given the features of battery power, the low energy consumption of WSNs has always been the center of attention as a major selling point. In general, the cost of energy may be broken down into two primary categories: the cost of transmission and the cost of sensing. When the identified target nodes break away from control, the sensing cost increases while the transmission cost remains constant. The second obvious difficulty is determining how to schedule the appropriate sensor nodes to reduce overall energy costs. Numerous researchers, including academics and engineers, have put forth a significant amount of effort to advance the target sensing capabilities of WSNs.

2. LITERATURE REVIEW

The estimate or prediction subsystem is the second component of the target tracking system. This component is responsible for carrying a prediction-based algorithm that is used to follow the moving route of the target. The redundant and varied data that is detected and sent by functional nodes is analyzed by prediction algorithms, which then extract useful information from the data. This subsystem is able to create the coordinates of the target that is now being localized. It then makes use of this information to extrapolate the target location in the subsequent tracking phase. After that, it systematizes the sensor network in order to monitor and keep a record of the moving route of the target.

The communication subsystem is the third component, and it is responsible for combining the estimations into a coherent position of the target. It also transmits the information that has been sensed from one node to another node, and it may also send the information to a centralized node known as the sink node for further processing. For the purpose of reducing the number of messages that are sent between nodes, this communication subsystem could have a tree topology or be based on clusters.

Target tracking is comprised of three subsystems, all of which collaborate with one another and remain in sync with one another in order to accomplish the task of localizing and tracking moving targets. Energy, overheads, and bandwidth are the examples of network resources that are used in order to follow and ensure that all of the subsystems of target tracking function as described. The achievement of equilibrium between the aforementioned network matrices is a demanding and complex task.

Among all of the sensor nodes that have been deployed, only a small number of the sensor nodes that make up the cluster are active at any one moment. Both static and dynamic clusters are possible. The moving target is detected and identified by sensor nodes within a cluster, and the data that is sensed is then sent to the cluster heads. Data is gathered from all of the members of the cluster by the cluster heads, who then locate the target and transfer the data to the sink node. It is the cluster head that is responsible for the aggregation of data since the members of the cluster are required to report the information that they have sensed to the cluster head rather than to the sink node. In the cluster-based target tracking strategy, there are many steps that include the construction of clusters, the selection of a cluster head, the aggregation of information, and the transmission of information to the Sink Node.

The deployment of sensor nodes in a wireless sensor network (WSN) might take the form of a hierarchical tree structure or a graph structure. The sensor node that is located in the closest proximity to the target is regarded as the root node of this tree. The other sensor nodes will be added or deleted in accordance with the movement of the target. As the distance between the root node and the destination increases, the pace at which the tree is reconfigured also increases. As a result of this, the tree-based tracking technique is not suitable for the tracking of objects that are moving at fast speeds. Because the outskirt nodes are constantly stimulated, it is possible that the energy stored in these nodes will be depleted in a short amount of time. It is necessary to make adjustments to this method in order to measure the accuracy of tracking since it is not extensible enough.

3. RESEARCH METHODOLOGY

FIRST PROPOSED LWKMTT MODEL

SYSTEM MODEL

- All of the sensors, together with a base station (also known as a sink), remain in place after deployment.
- Moving items that are being monitored in and around the region being monitored.
- The network field that is put on the grid has sensor nodes that are scattered uniformly across the field.
- As a result, sensor nodes that are powered by batteries have a restricted amount of power.
- The amount of energy that is still present in the sensor nodes may be calculated.

SECOND PROPOSED TRUST BASED TARGET TRACKING MODEL (TBTTM)

A two-step process is included in the proposed technique for tracking targets. The first stage involves the efficient selection of the Cluster head (CH), and the second stage involves the calculation of the trust level of the sensor node while the information about the target is being sent to the base station (BS). The clusters are produced in a dynamic way during the CH selection process, and the CH is selected for the first round of nodes that will function as CH. This process is known as the CH selection process. The algorithm known as LEACH is used in order to carry out this operation. After the data transmission has been finished, the residual energy of each node will be unique from that of the other nodes in the network. The reason for this is because sensor nodes consume a certain amount of energy for their operations. The rotation of the CH head takes place with each round, and the possibility of nodes in the cluster improving their chances of becoming CH is taken into consideration. The amount of power that nodes use is determined by a number of parameters, including sending and receiving, which are represented as. A comparison is made between the proposed system and TSR, and several network statistics, including the packet delivery ratio, the average end-to-end latency, and the energy usage, are analyzed.

EXPERIMENTAL ENVIRONMENT

According to the term reference, the Simulation may be defined as the replication of essential aspects of anything that is helpful in learning or preparing for something. At the most fundamental level, the cycle in which we are able to construct a single mathematical model is referred to as reproduction, and it is used to address the framework problem. This kind of interaction is often used in order to replicate the characteristics of the difficult task. In order to replicate the network in the same manner as portable impromptu networks such as MANET or VANET, there are a variety of test systems that may be used. Some examples of these systems are OPNET, Qualnet, and many more. The first half of this section will provide an overview of all of these networks, including their applications, as well as the benefits and drawbacks associated with utilizing them. For the purpose of our simulation, we need to choose one of them based on their availability and the degree to which they are compatible with the issue in order to mimic the task.

EVALUATION PARAMETERS

In order to legitimize both energy and quality of service efficiency, the exhibition of proposed steering protocols is estimated in terms of parameters such as normal delay, normal throughput, parcel conveyance proportion (PDR), normal energy utilization, and system lifetime. The meanings of the aforementioned parameters are elaborated upon below.

AVERAGE DELAY:

These measurements ascertain the normal time between the bundle start time at all sources and the parcel arriving at a time at all goal nodes.It is computed as:

$$D = \frac{\sum_{i=1}^{N} d_t^i + d_p^i + d_{pc}^i + d_q^i}{N} \quad (3.5)$$

Where N is number of total transmission links, d_t^i is transmission delay of i^{th}link, d_p^i is propagation delay of i^{th}link, d_{pc}^i is processing delay of i^{th}link, and d_q^i is transmission delay of i^{th}link.

AVERAGETHROUGHPUT

These measurements ascertain the absolute number of packets conveyed every second for example an all-out number of messages which are conveyed every second. The normal throughput Under Kbps is:

$$T = \left(\frac{R}{T^2 - T^1}\right) \times \left(\frac{8}{1000}\right) \quad (3.6)$$

Where R is complete received packets at all destination nodes, T^2 is simulation stop time and T^1 simulation start time.

Average Energy Consumption:

It computes the average energy consumption through entire network after the end of simulation through measuring the remaining consumed energy of all nodes. The total energy consumed $E^{tot}$is computed as:

$$E^{tot} = \sum_{i=1}^{N} E_i^{initial} - E_i^{consumed} \quad (3.7)$$

Where $E_i^{initial}$ and $E_i^{consumed}$ are initial and consumed energy of i^{th} node respectively. N is total number of nodes under network. The average consumed energy is computed as:

$$E^{avg} = \frac{E^{tot}}{N} \quad (3.8)$$

NETWORK LIFETIME

It estimates the total remaining lifetime that network will last.

Lifetime (Seconds) = Total Remaining Energy/10 (3.9)

PDR

It is the figuring of the proportion of the parcel got through the goals which are sent through the different wellsprings of the diverse traffic designs.It is computed as:

$$P = \left(\frac{P_r}{P_g}\right) \times 100 \quad (3.10)$$

Where, P_r are number of received packets and $P_g$number of generated packets?

4. DATA ANALYSIS

The assessment of the suggested scheme is covered in this part. Our approach aims to address the security concerns in target tracking based on dynamic clustering. We evaluate the suggested lightweight key generating scheme's performance in comparison to Localized Combinatorial Keying (LOCK), and we also analyze the nodes' energy usage. An event-driven simulator program called Network Simulator 2 (NS2) is used to conduct the simulation.

Figure 4.1 displays the packet delivery rate; when the percentage of dropped packets rises in response to malicious behavior, the suggested solution lowers the error rate by sending only authorized packets to their destinations.

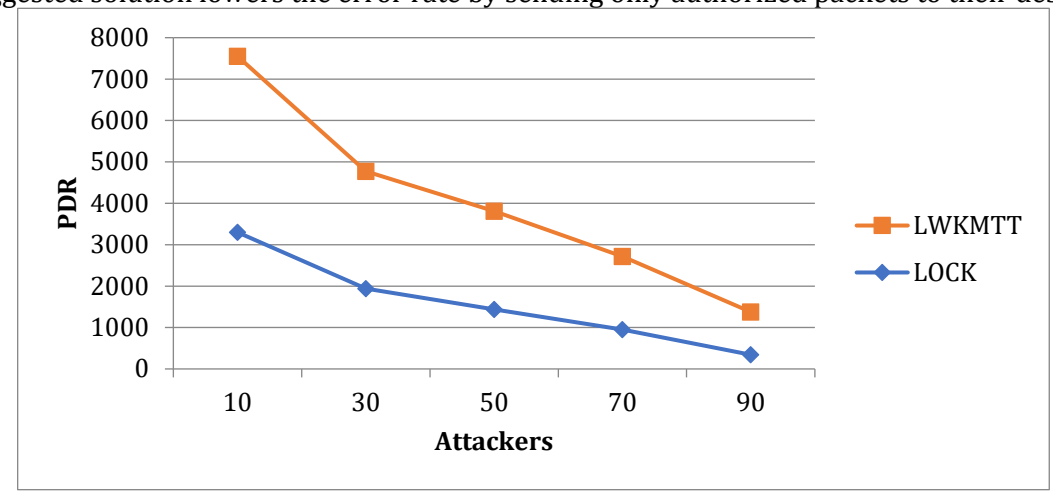

Figure 4.1: Packet Delivery Ratio, LOCK V/S LWKMTT

The correlation between the sensing range (tx) and the transmission range (rx) as a function of time is seen in Figure 4.2. There will be more static clustering if the transmission range is increased. When the $^{tx}/_{rx}$ decreases to a lower ratio, dynamic clusters are created.

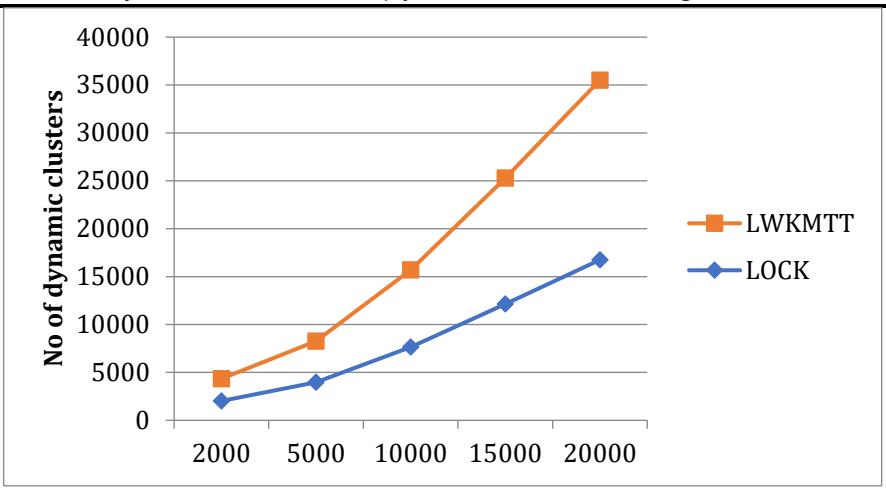

Figure 4.2: Dynamic Clustering LOCK V/S LWKMTT

The presence of malicious nodes in a network causes an increase in energy consumption, which in turn causes packet errors. Cluster heads save power by identifying rogue nodes and preventing incorrect messages from propagating over the network. Key generation node approach leads to increased energy consumption and network overhead in LOCK since the CH is responsible for generating and updating the key to the BS in response to target detection in the cluster area. The CH then distributes the key among its members.

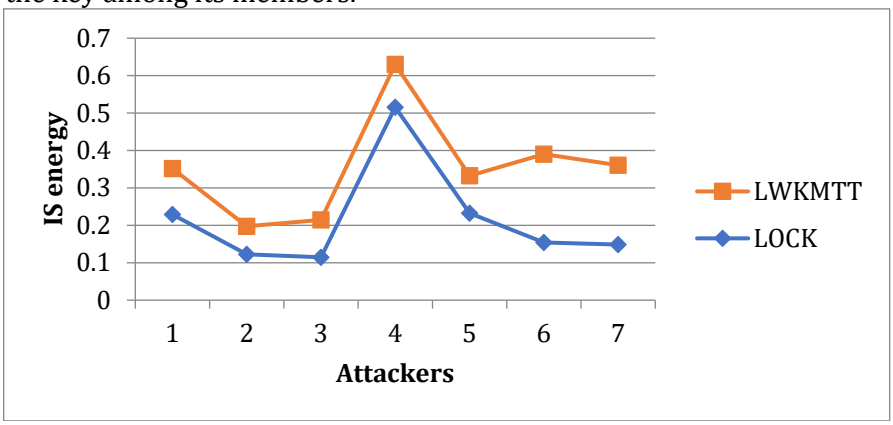

Figure 4.3: Energy Consumption, LOCK V/S LWKMTT

Here we compare the current TSR trust-based system with our 2nd proposed TBTTS scheme in terms of performance. For our investigations, we use the event driven simulation program (NS2) to test out various situations. Two kinds of attacks—the black-hole and the gray-hole—are the focus of the experiments. In a black hole network, the node willfully ignores control messages sent to it by other nodes, such as RREQ and RREP packets. By considering the node's trust level, the suggested TBTTS technique efficiently identifies black hole nodes. The routing process does not include a misbehaving node if its trust degree is less than a certain threshold. The malicious nodes in a gray-hole attack attempt to prevent data packets from reaching the base station (BS) by refusing to forward them and dropping them. All of the cluster members' trust degrees are sent to the cluster head (CH) using our trust mechanism. CH uses sensor recommendations to determine overall trust degree; however, the trust degree of the malicious node will be more than 0.5. We examine energy usage, average end-to-end latency, packet delivery ratio, and TSR, two network metrics, to see how the suggested strategy stacks up.

5. CONCLUSION

The majority of target tracking algorithms ignore security concerns in Favor of maximizing network lifespan via dynamic cluster formation. To prevent unauthorized parties from accessing sensitive information, security measures must be put in place for target tracking. Once an attacker has access to a node, it may trick BS into thinking it is doing anything harmful. This chapter proposes a secure trust-based target tracking strategy (TBTTS) that takes the trust level of one-hop sensors into account while sending data to BS in order to circumvent this issue. In order to detect rogue nodes, this approach aims to guarantee the data security of individual sensors by using a trust degree based on reputation. Additionally, the TBTTS system is compared to the trust-based routing method while dealing with nodes that have black

holes or Gray holes. Compared to TSR, TBTTS performs better in terms of energy usage, packet delivery ratio, and end-to-end latency.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

T. Khurana, S. Singh, and N. Goyal, "An evaluation of Ad-hoc routing protocols for wireless sensor networks," Int. J. Adv. Res. Comput. Sci. Electron. Eng., vol. 1, no. 5, pp. 27–30, 2012

A.S. H. Abdul-Qawy et al., "An enhanced energy efficient protocol for large-scale IoT-based heterogeneous WSN," Sci. African, vol. 21, pp. e01807, 2023.

K. Guleria, A. K. Verma, N. Goyal, A. K. Sharma, A. Benslimane and A. Singh, "An enhanced energy proficient clustering (EEPC) algorithm for relay selection in heterogeneous WSNs," Ad Hoc Netw., vol. 116, no. 3, pp. 102473, 2021

J. Wang, H. Han, H. Li, S. He, P. Kumar Sharma and L. Chen, "Multiple strategies differential privacy on sparse tensor factorization for network traffic analysis in 5G," IEEE Trans. Ind. Inform., vol. 18, no. 3, pp. 1939–1948, 2022.

M. Maheswari and R. A. Karthika, "A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks," Wirel. Pers. Commun., vol. 118, no. 2, pp. 1535–1557, 2021.

Y. Zhang and L. J. Gao, "Sensor-networked underwater target tracking based on grubbs criterion and improved particle filter algorithm," IEEE Access, vol. 7, pp. 142894–142906, 2019.

M. Anvaripour, M. Saif, and M. Ahmadi, "A novel approach to reliable sensor selection and target tracking in sensor networks," IEEE Trans. Ind. Inform., vol. 16, no. 1, pp. 171–182, 2020.

G. S. Kori and M. S. Kakkasageri, "Agent driven resource scheduling in wireless sensor networks: Fuzzy approach," Int. J. Inf. Technol., vol. 14, no. 1, pp. 345–358, 2022.

D. P. Bhagat, "Tracking of moving target in wireless sensor network with improved network life time using PSO," Wirel. Pers. Commun., vol. 127, no. 2, pp. 1225–1239, 2021.

H. Zhu, H. Chen, and M. Luo, "Adaptive event-driven robust set membership estimation for receivedsignal-strength-based moving targets localization," IEEE Internet Things J., vol. 9, no. 14, pp. 12825–12835, 2022.