International Journal of Multidisciplinary Education and Research
www.multieducationjournal.com
ISSN: 2455-4588
Received: 01-04-2024, Accepted: 02-05-2024, Published: 17-05-2024
Volume 9, Issue 2, 2024, Page No. 49-53

Efficient distributed multitarget tracking approach for WSNs for the performance improvement

Bukey Chetan Manikrao[1], Dr. Vijayalaxmi Biradar[2], Dr. Sagar B Shinde[3]
[1] Research Scholar, Department of Electronics Engineering, Kalinga University, Raipur, Chhattisgarh, India
[2] Department of Electronics Engineering, Kalinga University, Raipur, Chhattisgarh, India
[3] Professor, Department of CSE - Artificial Intelligence, PCETs NMVPMs Nutan Maharashtra Institute of Engineering and Technology , Pune, Maharashtra, India

Abstract
Aim of this study is to propose a multitarget tracking distributed approach with intelligent edge device using the AI. Task-oriented WSNs waste bandwidth. Communication for monitoring high-importance intrusion targets may be unreliable due to low bandwidth use. Sensor nodes' mobility and coverage may overlook or misinterpret crucial targets. Tracking accuracy may suffer. The central server's heavy compute demand slows tracing and prevents real-time control. Feedback may fail.

Keywords: Multitarget tracking**,** WSNs, task-oriented, AI, central server's

Introduction

In recent years, extensive research on a variety of sensing performances has yielded studies with outcomes that have been deemed adequate. However, present systems for the multi-target tracking of WSNs confront a great deal of difficulty in their implementation. Using Artificial Intelligence (AI), we will attempt this study work to present a novel multi-target tracking strategy for WSNs.

In a network, whether it is wired or wireless, there is a collection of devices that communicate with one another and exchange information and resources. These devices communicate with one another. It is essential for a device to have an interface in order for it to be able to connect with other devices; otherwise, the device will not be able to participate in an active network. Computers and other devices that are similar to computers, such as smart phones and palmtops, as well as other intelligent devices, are included in this category. These devices have a Network Interface Card (NIC) as an interface, which allows them to communicate with one another and complete the tasks that are necessary.

A wireless sensor network (WSN) is an example of an active network in which, in order to make a particular application operational, a collection of communication devices known as sensor nodes is deployed in either a systematic or random manner. These sensor nodes are physically a very small device that has a limited capacity for computation and communication. They are made up of a large number of hardware components and drivers that are associated with them. Miniature sensor nodes that are outfitted with a tiny battery that serves as a power source with a limited capacity, a sensing unit, a transceiver unit, and generally an integrated processing unit and storage. In addition to the infrared, acoustic, optical, seismic, magnetic, radio, biological, and chemical domains, the sensor node is able to accommodate one or more sensors that are capable of working in these areas.

The deployment of sensor nodes often takes place in a dense way and in a massive quantity. These sensor nodes that have been distributed are used for the purpose of measuring various physical phenomena in the detecting vicinity, including temperature, pressure, load, brightness, humidity, and wetness, among additional factors. The information that has been sensed is then sent to the centralised entity for the following process by means of the appropriate routing channel, and various control actions are carried out in accordance with the information. It is vital to keep both raw sensed data and processed data in a database since it is possible that both types of data may be needed at some point. The sensor field, sensor nodes, routing channel, central computing resource, data base, cloud computing resources, and remote computing resources are all included in this WSN scenario, which is presented in a very clear and concise manner.

Some of the areas of application include the automation of smart homes and offices, the monitoring of habitats, the detection of forest fires, the monitoring of hostile forces, crop monitoring in the field of agriculture, health monitoring, in industries to ensure the proper function of machines and the quality of the product that is being produced, traffic flow surveillance, asset tracking in warehouses, and smart cities, to name a few. Despite the fact that wireless sensor networks (WSN) have a limited battery capacity, a limited communication range of sensor nodes, and operational issues, they have gained widespread adoption in a variety of applications that have a significant impact on society and individuals in general.

Literature Review

A prediction-based method to target tracking is one that takes into account the moving trajectory of the target and makes predictions about its subsequent moving state. Only sensor nodes that have been activated in the network that has been constructed are utilized for tracking, while the other nodes stay in sleep mode in order to save energy. In spite of the fact that it is able to handle unexpected changes in direction with ease, it is unable to handle the fluctuating speeds of a moving object.

This method of tracking makes use of a spatiotemporal multicast protocol that is referred to as the Mobicast protocol. This protocol is responsible for distributing messages to a collection of sensor nodes that are placed in

specific zones that develop over time in an unanticipated way. There is no need for any previous knowledge on the movement pattern of the target while using the Mobicast protocol. The Mobicast protocol is a distributed technique for zone generation that is backed by collaborative sensors surrounding the target. It is based on the most recent updated kinematics parameters. In general, the term "Hybrid architecture" refers to the combination of the approach that was discussed before with the prediction mechanism. The use of heuristics is the foundation for prediction, and the estimation of the future state of a moving object is based on the perceived observation of its previous locations as well as the temporal and geographical information of sensors.

The ideal extraction of meaningful information about the status of the target from the observations is the most important factor in determining whether or not the target tracking operation is successful. Having a solid model of the target will unquestionably make the process of information extraction more simpler to a significant degree. One may claim without exaggeration that a decent model is worth a thousand pieces of data. This is a generic statement that can be generalized. This proverb has an even more powerfully positive meaning in the context of target tracking, which is characterized by very little observation data. Because a strong model-based tracking algorithm will significantly beat any model-free tracking algorithm if the underlying model turns out to be a good one, the majority of tracking algorithms are model-based. As a result, it is difficult to overestimate the significance of the function that a good model plays in this context.

If one does not have knowledge of the position of a sensor, the information that is supplied by that sensor is of little utility. The job of finding the position, such as the coordinates of a sensor or the spatial connections among objects, is referred to as localization. Since location is often unknown a priori, localization is the process of determining the position. In order to correctly offer information for useful applications that are aimed at localizing targets, it is essential to report the coordinates of sensor nodes. In addition to that, systems for information routing that are associated with location information are going to be used.

It is possible for localization systems to be classified into two primary categories, namely centralized and decentralized localization systems, depending on the communication that occurs between the nodes. For the purpose of computing the position of the target, centralized localization includes the use of sensed localization information that is then transferred to a central node. On the other hand, decentralized localization necessitates the transmission of the most recent coordinates of mobile targets via the use of hope, and it does not include the need of broadcasting each and every packet to a central node. As a result, decentralized localization approaches have a lower power usage compared to centralized techniques. The centralized localization technique has two advantages over the decentralized localization technique, as stated by. The first advantage is that sensor nodes are not required to have good processing potential. The second advantage is that the mobility and abnormality of the mobile target requires recurrent data communications between nodes in order to achieve superior localization accuracy. This eliminates the primary advantage of the decentralized localization technique.

Research Methodology

A wireless sensor network is made up of very small sensors that are low in weight and have a limited battery supply. These sensors are able to detect physical events and then report them wirelessly to a sink or BS. Widespread uses of wireless sensor networks (WSN) have highlighted significant challenges in terms of delivering energy efficiency and security. These applications include monitoring and target tracking. When it comes to large-scale wireless sensor network applications, such as mission-critical networks, ensuring network security and prolonging network lifespan is a crucial concern. The absence of physical protection allowed attackers to gain access to the node, which resulted in the generation of misleading information about the monitored target and the provision of inaccurate estimations regarding the moving target. In order to safeguard against harmful actions, the monitoring of targets requires the provision of secure communication and the protection of their privacy protections.

Research purpose

Purpose of this study is to design the novel distributed multitarget tracking algorithms for performance improvement in WSNs.

Research design

This study will cover title of the study, significance of the study, aims and objectives of the study, research hypothesis and research design. This research has designed based upon descriptive study as it aims an in-depth analysis on relationship standard methods in multitarget tracking in WSNs. The research design contains the following steps:

Theoretical and experimental analysis

Consequently, the following **hypothesis** will be invented:

H1: There is direct relationship between target tracking and WSN-based application performances.

H2: There is direct relationship between multitarget tracking and performance improvement in WSN.

H3: There is direct relationship between the sensing-based multitarget tracking algorithm and performance efficiency.

Data collection

This study is based on secondary research method. Thus, gathering and analyzing the data will be done on the basis of existing research.

Tools and techniques

In this research work we will use simulation tools to implement and evaluate the proposed models with existing methods.

1. We will use a detailed simulation model based on NS.
2. We will use the different metrics to compare the performance of proposed methods.

Analysis and interpretation

Every one of the models will undergo simulation and evaluation on a 64-bit version of Windows 11 equipped with an Intel I5 CPU and 8 gigabytes of random-access memory. The proposed and existing models will be implemented and evaluated using the different WSN network scenarios and conditions.

Average Delay: This metrics calculates the average time between the packet origination time at the all sources and the packet reaching time at the all-destination nodes. It is computed as:

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

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: This metrics calculates the total number of packets delivered per second i.e. total number of messages which are delivered per second. The average throughput in Kbps is:

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

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 by entire network after the end of simulation by measuring the remaining consumed energy of all nodes. The total energy consumed E^{tot} is computed as:

$$E^{tot} = \sum_{i=1}^{N} E_i^{initial} - E_i^{consumed} \quad (3)$$

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

$$E^{avg} = \frac{E^{tot}}{N} \quad (4)$$

E. Network Lifetime

Lifetime (Rounds) = Total Remaining Energy/10

PDR: It is the calculation of the ratio of packet received by the destinations which are sent by the various sources of the different traffic patterns. It is computed as:

$$P = \left(\frac{P_r}{P_q}\right) \times 100 \quad (5)$$

Where, P_r is number of received packets and $P_q$number of generated packets.

Communication Overhead: It is computed as the ratio of total number of routing packets to the total number of data packets in network. It is computed as:

$$O = \sum_t \left(\frac{RT^t}{DT^t}\right) \quad (6)$$

where, $RT^t$is total number of routing packets and DT^t is total number of data packets at time t.

Data Analysis

Our technique chooses efficient cluster neighbors to send data to BS in order to reduce the impact of harmful network activity. Compared to the current TSR trust-based method, which fails to withstand the presence of malicious nodes and provides inaccurate predictions (as seen in Figure 1 of the PDR graph), TBTTS performs better.

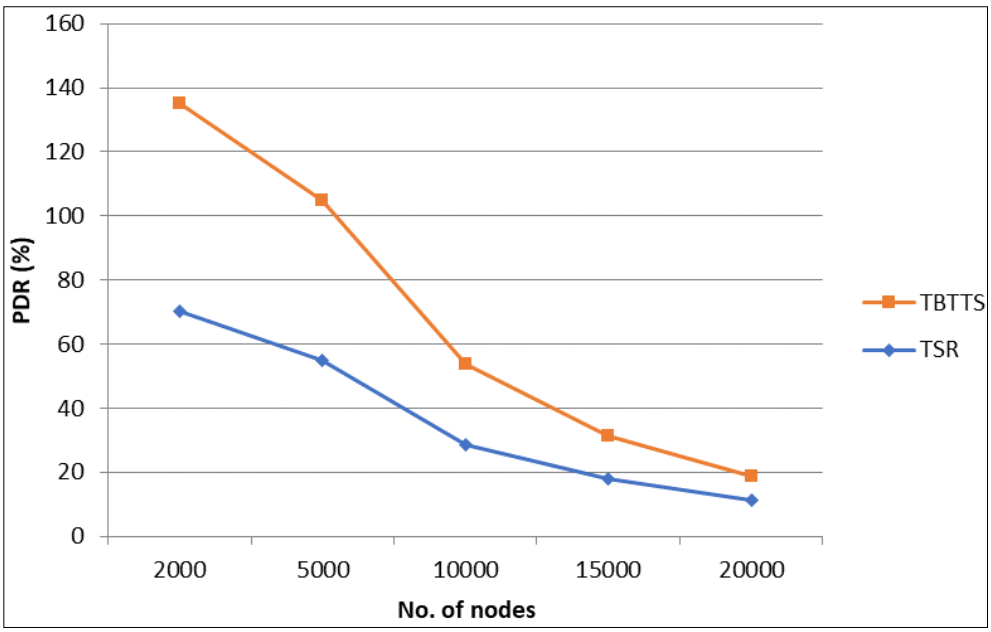

Fig 1: Packet delivery ratio, TSR V/S TBTTS End-to-End Delay.

Our approach detects hostile nodes and avoids them when routing data packets, minimizing latency (as shown in Figure 2 of the average end-to-end delay graph).

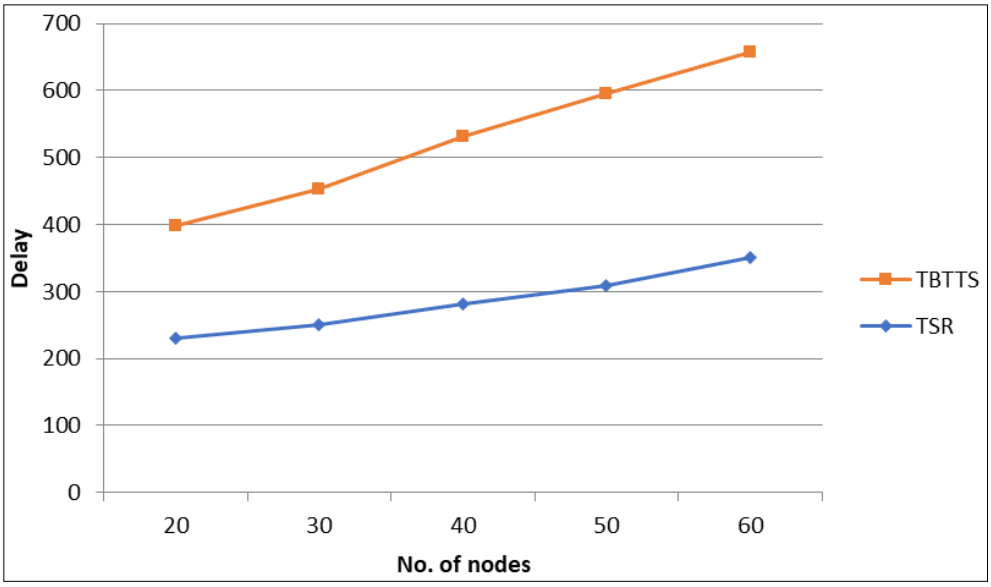

Fig 2: Average end to end delay, TSR V/S TBTTS

More power is used as a result of the sensor retransmitting data to CH when malicious nodes are present. By switching nodes to CH and balancing their energy output, our strategy extends the life of the network". By using better cluster head rotation and updating residual energy, TBTTS extends the lifespan of networks, as shown in Figure 3, in comparison to the current TSR trust-based system.

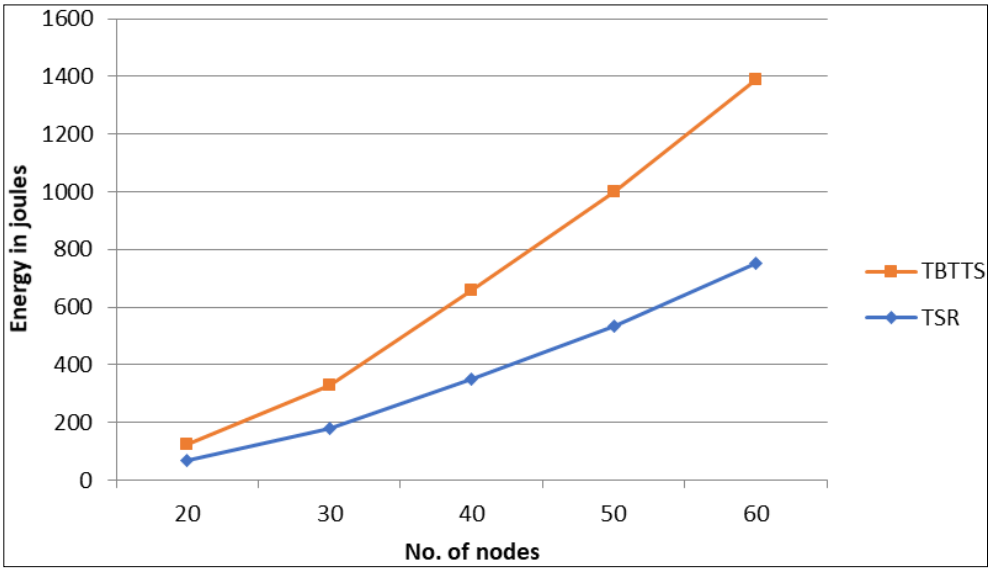

Fig 3: Average energy consumption, TSR V/S TBTTS

Conclusion

Avoiding harmful network activity and increasing network rate even while attackers are present is the goal of the first suggested LWKMTT method. The suggested method has the ability to update keys in order to identify compromised nodes and can retrieve concealed keys from nodes prior to distribution. Degradation of the network occurs when LOCK re-uses the key to insert more malicious nodes. One major limitation of WSN is the potential for malicious behaviour to compromise nodes and attempt to drain their energy. Improving the network's overall efficiency is possible via authentication and protecting it from harmful activity. Dynamic cluster formation occurs and CH is produced while the monitored moving object travels randomly. After receiving the target tracking information from the BS, the CH verifies their identity using lightweight key management. By effectively identifying and preventing malicious behaviour, the suggested technique decreases the nodes' overhead and delivers packets efficiently. Protecting WSN target tracking apps from attackers is a difficult problem.

Reference

1. Chauhan P, Ahlawat P. Target tracking in wireless sensor network. Int J Inf Comput Technol,2014:4(6):643-648.
2. Rezaee AA, Namazi Nik A. Particle filter-based target tracking in wireless sensor networks using support vector machine. Comput Knowl Eng,2018:1(2):13-20.
3. Khan MW, Salman N, Ali A, Khan AM, Kemp AH. A comparative study of target tracking with Kalman filter, extended Kalman filter and particle filter using received signal strength measurements. In: Emerging

Technologies (ICET), 2015 International Conference on. IEEE, 2015.
4. Gao W, Zhao H, Song C, Xu J. A new distributed particle filtering for WSN target tracking. In: International Conference on Signal Processing Systems, IEEE, 2009. 334-337.
5. Coates M. Distributed particle filters for sensor networks. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, 2004, 99-107.
6. Li D, Wong KD, Hu YH, Sayeed AM. Detection, classification, and tracking of targets. IEEE Signal Process Mag,2002:19(2):17-29.
7. Hlinka O, Hlawatsch F, Djuric PM. Distributed particle filtering in agent networks: a survey, classification, and comparison. IEEE Signal Process Mag,2012:30(1):61-81.
8. Hsu CW, Chang CC, Lin CJ. A Practical Guide to Support Vector Classification, 2003.
9. Jondhale SR, Mohan V, Sharma BB, Lloret J, Athawale SV. Support vector regression for mobile target localization in indoor environments. Sensors,2022:22(1):358.
10. Bhatti G. Machine learning based localization in large-scale wireless sensor networks. Sensors,2018:18(12):4179.