I J C T A, 8(5), 2015, pp. 2219-2227

Intrusion Detection Framework for Object Tracking in Wireless Sensor Networks

Gauri Kalnoorá, Jayashree Agarkhed[2], Siddarama R. Patil[3]

Abstract: A wireless sensor network (WSN) comprises of spatially distributed inexpensive, tiny sensors which monitor physical or environmental conditions such as forest fire, pressure, temperature, humidity, object movement etc., in a collaborative manner. Tracking of an object becomes most important application, as it moves through the sensor network.Some of the applications in WSN need to be secured and are critical.Thus, we have discussed the application framework of object tracking for detecting an intruder in WSN.

1. INTRODUCTION

In WSN [1], set of sensor nodes are deployed spatially and they are capable of maintaining a wireless communication channel and don't rely on any infrastructure that is fixed. The communication channel exists between each other. This differentiates the wireless networks from wired networks substantially. And there is no single point of access that exists with the wireless network where all the nodes should cooperate with each other and creates the entire network for setting up its own infrastructure (for e.g. a subsystem for routing) and also services such as collection of data. Finally, most of the operations of nodes are to be carried out in a spatially distributed manner. In recent years, huge numbers of efforts in research have been made for developing sensor hardware with architectural network in order to deploy WSNs effectively for a many type of applications. Parameters of network mainly related to range sensing, transmission, and also node density that have to be considered carefully at the stage of network design, according to specific applications. This can be achieved which is critical for capturing the impacts of different parameters of a network based on the network performance with respect to application specifications. Mainly considering military applications, the development of the sensor networks was motivatedoriginally, such as battlefield surveillance. WSNs however are majorly now used in many civilian application areas, that includesmonitoring of environment and habitat, healthcare applications, traffic control and home automation. Inthe past few years, growth in research has been most explosive that is devoted in the field of WSN, a wide range of areas are covered, which extends to advancement technologically from understanding the issues theoretically.This has made such network realization possible.

Such networks has collection of hundreds and thousands of wireless sensor nodes (motes) that are inexpensive and monitoring of certain phenomena in wide areas, capturing some distinct measurements geographically over a long period of timeThese motes are characterized with limited resources for example, storage, communication and computational capabilities.The most pervasive interconnection of these devices has created broad class of real exciting and new applications in several real time areas mainly that includes healthcare applications, traffic control and so on. In everysensor network, however,the motes are exposed to other security threats that which with, if notaddressed properly, then they can be excluded to be deployed in thescenarios that are envisaged [2].

[2,3] P.D.A. College of Engineering, Kalaburagi, Karnataka–585102, India. *Email: ákalnoor.gauri@gmail.com, jayashreeptl@yahoo.com, pdapatil@gmail.com*

In military applications, the motes in WSNs and WSNs as entirety are dispersed into a harmful adversary's territory especially for detecting and tracking thesoldier's enemy and vehicles. In other few indoor environments, these sensor networks are spatially deployed to detect intruders through a wireless home security system. Considerably, WSNs are networks that are most probably unattended but reachable physically from the outside world, so that they are vulnerable to many security threats and attacks. Thus, WSNs need to be prevented from an intruder and also must be secured from obstructing the delivery of real sensordata and preventing from forging the sensor data.

2. RELATED WORK

Survey on intrusion detection and prevention is enormousand also few measures in WSN have been carried out in recent years that deal with security threats.

Authors in [3] propose Intrusion Detection in Homogeneous andHeterogeneous WSNs. Introduction to WSN and the deployment of wireless sensors is discussed.In [4], authors have proposed the multiple-sensing detection technique. In [5], [6], [7], [8], the authors have showed that thelocality of an intruder can be determined only from at least three sensors' sensing data.Authors in [9] proposes an anomaly approach of detectionthat is based on self-organized criticality (SOC) and Hidden Markov models to detect inconsistencies in data. This approach is developed based on the structure with events that are naturally occurring. With the gained knowledge that is distilled from the criticality aspect for self-organized deployment region, this applies a hidden Markov model. This lets the adaptation of sensor networks with the norm in its natural surrounding and environment so that any unusual activities can be singled out.

Authors in [10] formulate and propose the defense of attack problem by using game theory and Markov Decision Process to detect or predict the possible vulnerable motes. They have formulated the problem as a nonzero-sum, two-player and a non-cooperative game that may exist between an attacker and WSNs.Nash equilibrium is achieved with this game leading to a strategy of defense for the network [11]. Later on, a Markov Decision Process is usedfor prediction of attacks.Finally, an intuitive metric (node's traffic) is used and the node that has the highest value of this metric is being protected.

Some articles provide intrusion detection techniques, apart from the general approaches, for particular operations. In [12], a distributed algorithm is described, known as BOUNDHOLE, and it builds routes around the holes of routing, which are regions of the networkconnected with boundaries that consists of all thenodes that are stuck. In geographic routing it is shown that hole-surrounding routes, informationstorage mechanisms, path migration, and identification of regions ofinterestcan be used. Author in [13] proposes a general scheme for detecting localization of anomalies normally that are harmed and caused by adversaries. The problem as an anomaly intrusion detection is formulated, and a number of ways isproposed to detect localization anomalies.

In [14], an intrusion detection technique is described that uses information about thetopology of network and also the positioning of sensors particularly to determine malicious kind of attack in a particular area of the network. This technique relies on an algorithm that generates the appropriatesignatures of sensors automatically. This approachis applied to an intra-domain distance-vector protocol and reports the results of its evaluation.Moreover, there are few articles that applies fault-tolerant technologies for providing security to network. In [15], to provide intrusion tolerance, a secure multi-pathroutingis designed to multiple destination base stations which are against isolation of a single base station. Also, few strategies of anti-traffic analysis are proposed to help from eavesdroppers bydisguising the location of the base station.

The technique in [16] mainly targets and aims the identification of faulty sensors and also the detection of events reachability with faulty sensorsin sensor networks. It has proposed two algorithms as identification of faulty motesanddetection offault-tolerantevent boundary. These algorithmsare scalable andlocalized for WSNs.

In this article, we will discuss about issues and challenges of security in WSN and also we propose our intrusion detectionframework for WSN. We aim at developing novel and effective mechanisms for tracing the attackers on WSNs whichadapt to thenetwork features.

3. PROPOSED WORK

Following section describes the design issues of WSN andIDS framework for detecting an intruder by tracking an object.

3.1. Design issues

The design issues of WSN are a major factor. WSN is designed with four major securityparameters.

Confidentiality: Informationbetween sender and receiveronly must be shared and should not be leaked to or shared with a third party that is not authenticated.

Integrity: Integrity of information is said to be maintainedonly when there is no change in the data eitherin form or in meaning.

Availability: Information should be available whenever required to the authentic sender and the receiver to read and process it.

Authenticity: The produced information or that is already with the sender and the receiver should be verified if it is original and correct, that means the information shared should be authentic or verifiable and should also hold some meaning. The sender should be able to verify the originality of the receiver and vice versa.

3.2. IDS Framework

The framework designed for detecting an intruder is discussed in this section. The framework is designed in such a way that it can detect the intrusions,react to the intrusions, and locate the attackers. It is composed of three parts, intrusion detection, intrusion tracing, and reaction of intrusion. Figure 1 shows the intrusion detection frameworkthat adapts to the environment of WSN.

These three proceduresare performed one after another.

Firstly, intrusion detection will be performed.The intrusion detection process will detect the intrusions in the network bysensing any suspicious phenomenon from the audit data. Once if an intrusion is detected

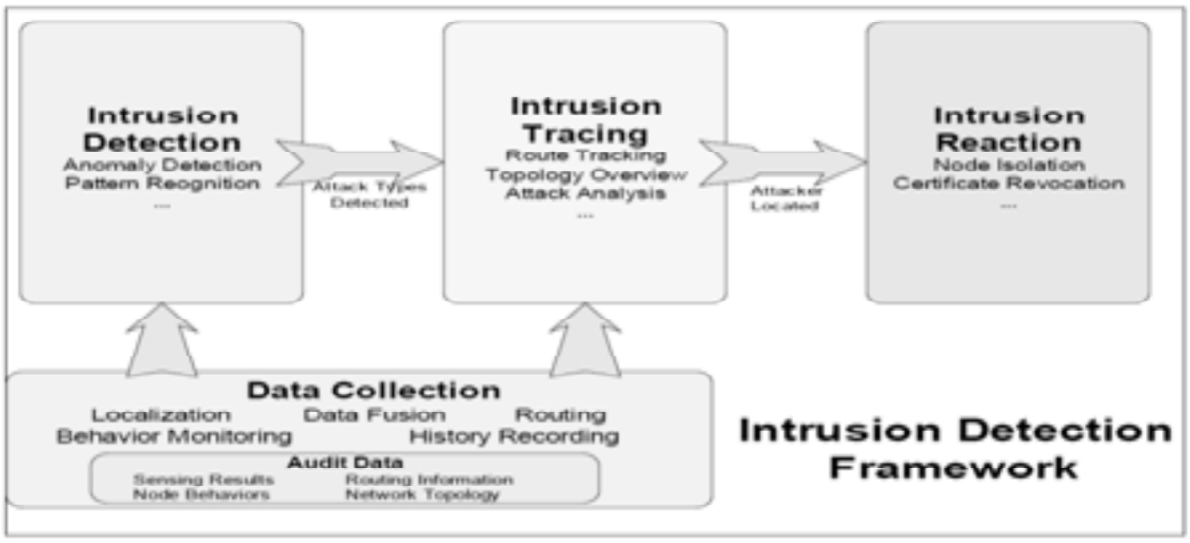

Figure 1: IDS Framework

on the network, classification is done on what type of attack it belongs to. Some of the traditional mechanisms for detecting an attack are anomaly detectionand pattern recognition.We will investigate new methods to collect relevant audit data and detect intrusions especially for wireless sensor networks. Intrusion tracing is an important process in our intrusion detection framework.

If intrusions exist, then intrusion tracing will be executed so that it can locate the attacks. In addition to sensing an intrusion, we work further to identifyand locate the attack.Intrusion reaction is the final stage in this IDS framework. Itsmain purpose is to defend against the attacks after discovering, classifying, identifying, and locating the attacks.Traditional methods for this kind of protection include node isolations and certificate revocations.

3.3. Flow Diagrams

There are five modules in the proposed method and are discussed in this section.

Constructing Sensor Network: Each node is connected to the neighboring node and it is independentlydeployed in the network area and each port number is authorized in a node (Figure 2).

Packet creation: In this module, we browse and select the source file. And the selected data is converted into fixed size of packets. The packetsare sent from source to detector (Figure 3).

Finding authorized and unauthorized port: In this module, we browse and select the source file. And the selected data is converted into fixed size of packets. The packetsare sent from source to detector (Figure 4).

Constructing inter-domain Packet filters: If the packet is received from other than the port no, it will

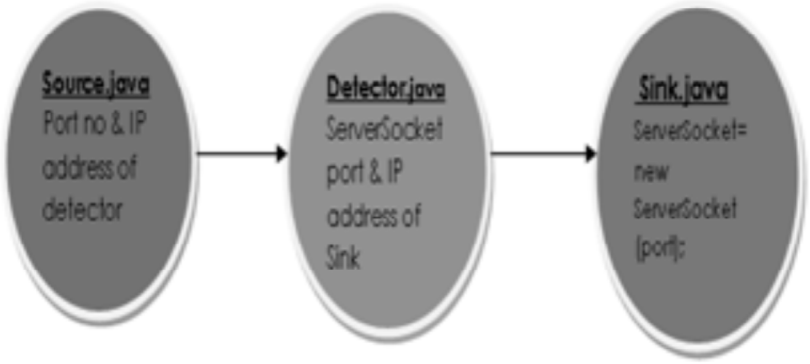

Figure 2: Sensor Network Construction

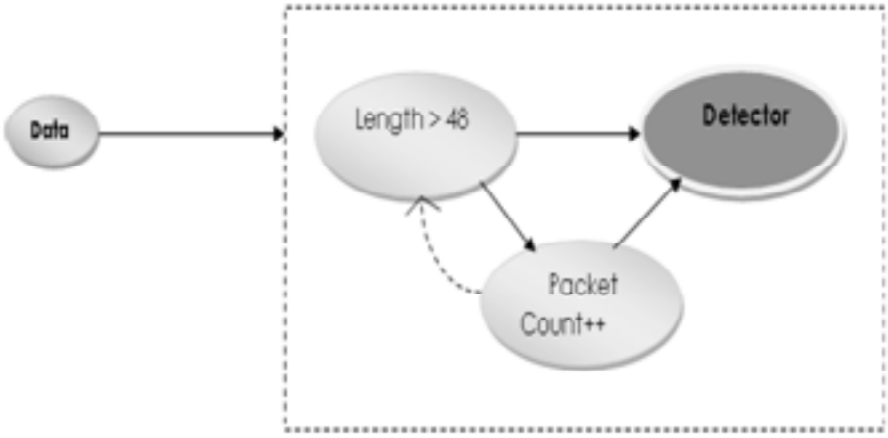

Figure 3: Packet Creation

be filtered and discarded. This filter only removes the unauthorizedpackets and the authorized packetsare sent to the destination(Figure 5).

Receiving the valid packet: Here, after filtering invalid packets, all valid packets willreach the destination (Figure 6).

4. RESULTS AND DISCUSSIONS

In this section, the results in terms of snapshots of proposed method are presented.Network simulations were performed bydeveloping a discrete-event object-oriented network simulator in java.

4.1. Simulation Results

Packets received at the detector (receiver) from an authorized port are forwarded to sink (Base station).

5. CONCLUSION

In this work, we have introduced WSN and its security issues. To address the security issues, we studied intrusion detection measures and discussed our research direction. We propose an intrusion detection

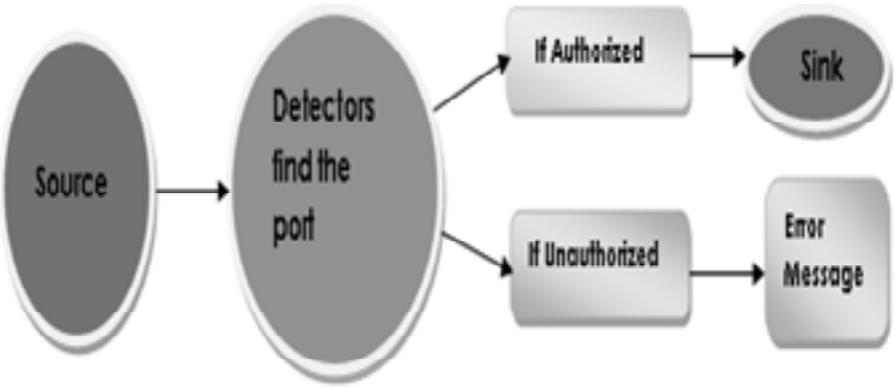

Figure 4: Port Search

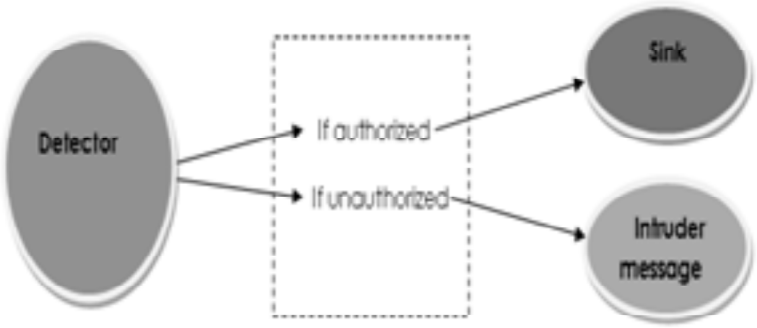

Figure 5: Constructing Inter Domain Packet Filters

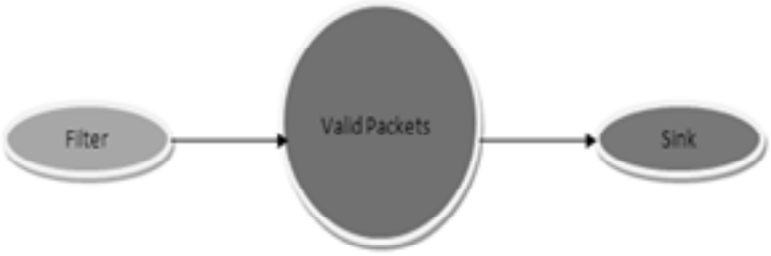

Figure 6: Receiving valid packet

Figure 7: Source

Figure 8: Message from source

Figure 9: Packets Creation at source

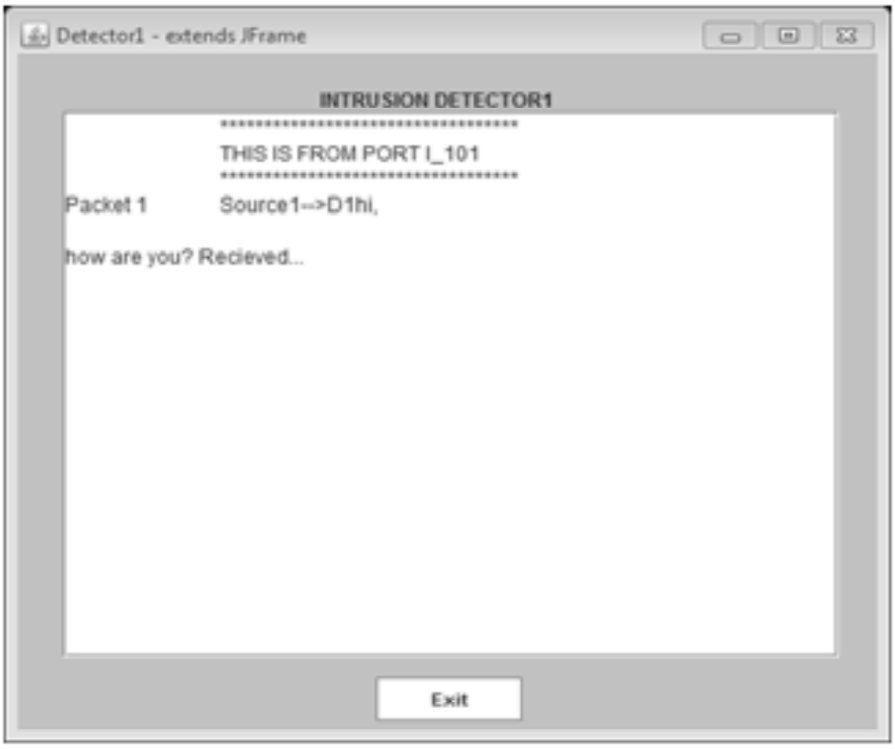

Figure 10: Detector-Receiver receiving packets from source

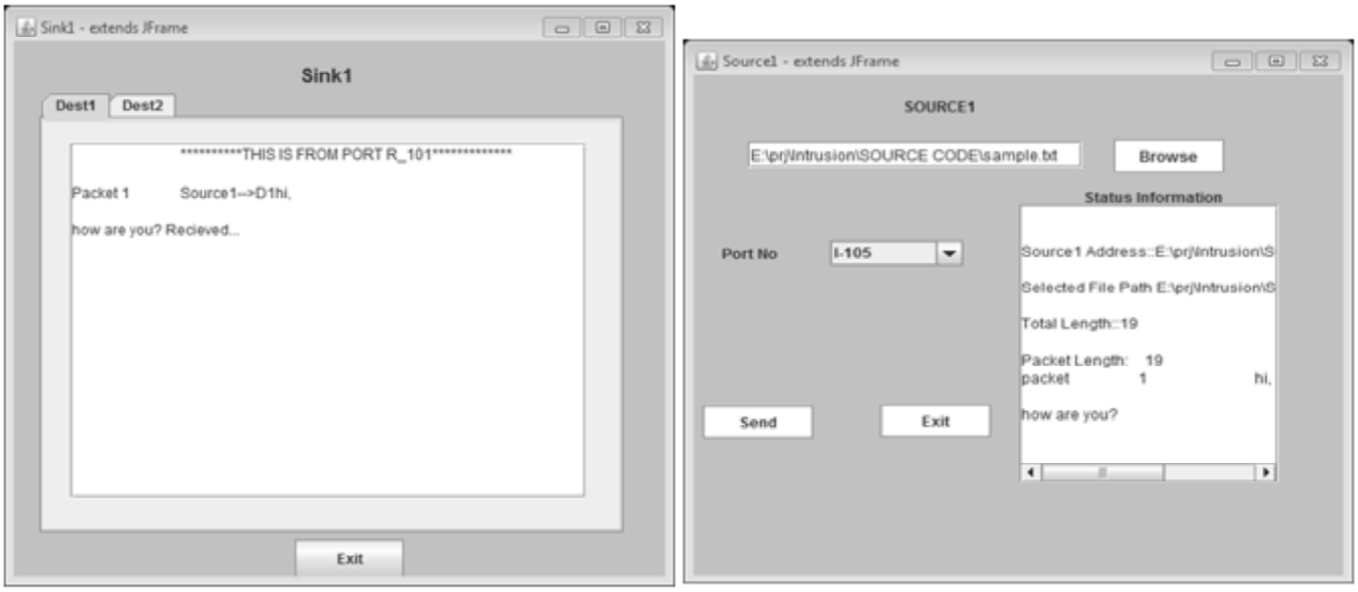

Figure 11: Source Detector Detecting the intrusion

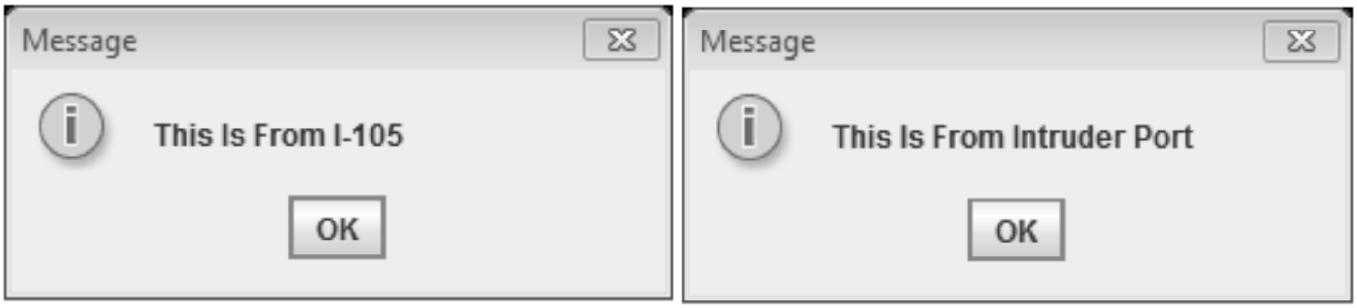

Figure 12: Source Detector Detecting the intrusion

Figure 13: Sink: Source sending the file through unauthorized (intruder) port

framework which can detect the intrusions, trace the intruders, and resist against the intrusions on wirelesssensor networks. Our framework contains various detection components for collecting audit data. A number of techniques are considered for analyzing the data. After detecting and classifying the intrusions, our tracing procedure will attempt to identify and locate the intruders. Finally, resistance measureswill be employed to defend against the intrusions. We analyzed the properties of a number of attacks on WSNs. Then, we proposed two intrusion detection architectures for hierarchical and cell-based wireless sensor networks.

References

[1] Ma, S. S., Qian, J., & Sun, Y. (2013), Optimal sleep scheduling scheme for wireless sensor networks based on balanced energy consumption. Journal of Computers, 8(6), 1610-1617.

[2] Ramya, K., Kumar, K. P., &Rao, V. S. (2012), A survey on target tracking techniques in wireless sensor networks. International Journal of Computer Science and Engineering Survey, 3(4), 93.

[3] Daoudi, A., Kerfi, Y., Benelallam, I., &Bouyakhf, E. H. (2012), Multi-objective optimization approach for wireless sensor networks deployment in three dimensional environments. Journal of Electronic Systems Volume, 2(3), 127.

[4] Xu, X., Huang, L., He, J., Huang, H., & Jiang, G. (2013), A fine-grained hop-count based localization algorithm for wireless sensor networks. Journal of Computers, 8(3), 567-575.

[5] Wang, S. H. (2013), An exchange framework for intrusion alarm reduction in mobile ad-hoc networks. Journal of Computers, 8(7), 1648-1655.

[6] Akewar, M. C., & Thakur, N. V. (2012), A study of wireless mobile sensor network deployment. Internatioal Journal of Computer and Wireless Communication, 2(4).

[7] Wang, Z., Lou, W., Wang, Z., Ma, J., & Chen, H. (2013), A hybrid cluster-based target tracking protocol for wireless sensor networks. International Journal of Distributed Sensor Networks, 2013.

[8] Jiang, B., Ravindran, B., & Cho, H. (2013), Probability-based prediction and sleep scheduling for energy-efficient target tracking in sensor networks. Mobile Computing, IEEE Transactions on, 12(4), 735-747.

[9] Li, X., Ci, L., Yang, M., Tian, C., & Li, X. (2012), Deploying three-dimensional mobile sensor networks based on virtual forces algorithm. In Advances in Wireless Sensor Networks (pp. 204-216). Springer Berlin Heidelberg.

[10] Shoaee, S., &Haghighat, A. T. (2013), An Efficient Protocol for Target Tracking in Wireless Sensor Networks (WSNs). Advances in Computer Science: an International Journal, 2(5), 13-19.

[11] Guo, M., Olule, E., Wang, G., &Guo, S. (2010), Designing energy efficient target tracking protocol with quality monitoring in wireless sensor networks. The Journal of Supercomputing, 51(2), 131-148.

[12] Khajei, R. P., &Ghatei, S. (2011), An Extensive Study on Base Station Based Target Tracking in WSNs. International Journal of Simulation—Systems, Science & Technology, 12(2).

[13] Padmanabhan, K., &Kamalakkannan, P. (2012), Energy-efficient dynamic clustering protocol for wireless sensor networks. International Journal of Computer Applications, 38(11).

[14] Shoaee, S., &Haghighat, A. T. (2013), An Efficient Protocol for Target Tracking in Wireless Sensor Networks (WSNs). Advances in Computer Science: an International Journal, 2(5), 13-19.

[15] Guo, M., Olule, E., Wang, G., & Guo, S. (2010), Designing energy efficient target tracking protocol with quality monitoring in wireless sensor networks.*The Journal of Supercomputing*, *51*(2), 131-148.

[16] Padmanabhan, K., & Kamalakkannan, P. (2012), Energy-efficient dynamic clustering protocol for wireless sensor networks. International Journal of Computer Applications, 38(11).