International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-9, Issue-3, June 2022
https://doi.org/10.55524/ijirem.2022.9.3.25
Article ID IJIRP-1201, Pages 162-166
www.ijirem.org

Exploitation and Incursion Finding Approach in Various WSW

Dr. A. Seshagiri Rao[1], K. Manohara Rao[2], and M. Sivudu[3], and Dr. Patan Hussain Basha[4]

[1]Professor, Department of Information Technology, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India
[2,3]Assistant Professor, Department of Information Technology, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India
[4]Associate Professor, Department of Computer Science & Engineering, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India

Correspondence should be addressed to Dr. A. Seshagiri Rao; ithod@pace.ac.in

ABSTRACT- Incursion finding is a process of identifying and responding malicious activity. Wireless sensor webs consisting bulk of ‘ sensors’ are useful to integrate data in variety of environment. The basic sensors are simple and have limited power supplies. Heterogeneous wireless sensor webs are better scalable and lower overall cost than homogeneous sensor webs. In this paper, we are improving the lifetime of wireless web and we present a survey of various energy efficient techniques in a various wireless sensor web. It is important to improving wireless web because sensor nodes in wireless webs are constrained by limited energy.

KEYWORDS- Energy efficient, different wireless-web, homogeneous wireless web, Incursion finding, Wireless sensor web, sensors,

I. INTRODUCTION

Wireless sensor web (WSW) refers a structure that having of digit of inexpensive, resource limited sensor nodes to intellect significant information linked to surroundings and convey it to descend knot that provides entry methodology to one more web, or an entrée for individual. WSW is a speedily increasing region as novel technologies are budding; upcoming apps are being urbanized, such as travel, surroundings monitor, healthcare, forces applications, and home computerization. WSW is vulnerable to various attacks such as jamming, battery drainage, routing cycle, cloning. Due to limitation of computation, memory and power resource of sensor nodes, omplex security mechanism cannot be implemented in WSW. Therefore energy-efficient security implementation is an important requirement for WSW.

In homogeneous webs all the sensor nodes are identical in terms of battery energy and hardware complexity. With purely static clustering (cluster heads once elected, serve for the entire lifetime of the web) in a homogeneous web, it is evident that the cluster head nodes will be overloaded with the long-range transmissions to the remote base station, andthe extra processing necessary for data aggregation and protocol co-ordination. As a result the cluster head nodes expire before other nodes. However it is desirable to ensure that all the nodes run out of their battery at about the same time, so that very little residual energy is wasted when the system expires.

On the other hand, in a heterogeneous sensor web, two or more different types of nodes with different battery energy and functionality are used. The motivation being that the more complex hardware and the extra battery energy can be embedded in few cluster head nodes, thereby reducing the hardware cost of the rest of the web. Thus there are two desirable characteristics of a sensor web, viz. lower hardware cost, and uniform energy drainage. While heterogeneous webs achieve the former, the homogeneous webs achieve the latter. However both features cannot be incorporated in the same web.

An Incursion Finding System (IDS) finds a safety abuse method by observation and scrutiny the web activity. Two methods: misuse finding and anomaly finding. ‘Misuse’ finding identifies an unofficial use from signatures while irregularity verdict identifies from analysis of an event. When both techniques detect violation; they raise an alarm signal to warn the system. Incursion finding is analyzed in two scenarios: single sensing finding and multiple sensing finding .In single sensing finding the intruder is detected by a single sensor. But at least three sensors should detect the intruder in a

collaborative manner to find out the exact location of the Intruder. Therefore we have analyzed the multiple sensing finding too. We derive the expected incursion distance and evaluate the finding probability in different application scenarios. we theoretically capture the impact on the finding probability in terms of different web parameters, including node density, sensing range, and transmission range.

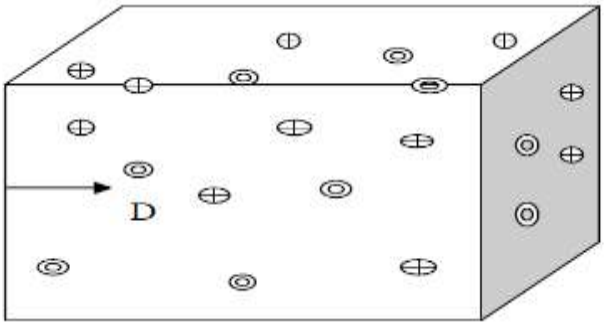

Figure 1: Distance moved by intruder

II. HETROGENEOUS WSW

A typical heterogeneous wireless sensor webs consists of a large number of normal nodes and a few heterogeneous nodes. The normal node, whose main tasks are to sense and issue data report, is inexpensive and source-constrained. The heterogeneous node, which provides data filtering, fusion and transport, is more expensive and more capable. It may possess one or more type of heterogeneous resource, like for e.g. enhanced energy capacity or communication capability. Their batteries may be replaced easily. Compared with the normal nodes, they may be configured with more powerful microprocessor and more memory. They also may communicate with the sink node via high-bandwidth, long-distance web, such as Ethernet. If heterogeneous node is present in WSW then it can increase web reliability and lifetime.

A. Exploitation

In heterogeneous sensor webs, the basic sensors can be deployed randomly as in homogeneous sensor webs. The cluster heads, on the other hand, should be more carefully deployed to make sure all basic sensors are covered, that is, each sensor can hear from at least one cluster head. However, since the number of cluster heads is small, their best locations can be found within a reasonable amount of time and they can even increase their transmission
power to cover remote sensors. The problem of sending packets from sensors to a single sink node with energy constraints has been studied. However, the difference between our work and those is profound. First, assume that data should be gathered by a data-forwarding tree, that a tree is not the best structure for data gathering applications. The best structure can be found by running a web flow algorithm, which is what we will adopt in our work. Second, in essence, focus on traffic routing, whereas we consider both traffic routing and media access control.
In this paper, an Intruder is defined as any moving object that enters into the WSW area .It may enter from a random point, or through boundary of the exploitation area. If dropped from the air then the entry point can be considered as a random point. We present the analysis of incursion finding in a heterogeneous WSW.

B. Types of Resource Heterogeneity

1)Computational Heterogeneity

A heterogeneous node has more complex processor and memory so that they can perform sophisticated tasks compared to a normal node.

2)Link Heterogeneity

A heterogeneous node possesses high bandwidth and long distant transceiver than a normal node proving reliable transmission.

3)Energy Heterogeneity

A heterogeneous node is line powered (its battery is replaceable).Out of the above the energy heterogeneity is the most important, since computation and link heterogeneity consumes more energy.

4)Impact of Heterogeneity on WSW

Placing heterogeneous nodes in the sensor web, decreases response time and improve battery life time. As discussed above, Computation and link heterogeneity decreases the waiting time thereby, decreasing the response time. The average energy consumption will be less in heterogeneous sensor webs for forwarding a packet from the normal nodes to sink, hence life time is increased.

III. INCURSION FINDING SYSTEM

Event Data is the web activities (for example number of success and failure of authentication). Alert is an interface between operating system and IDS. Duties of alert are broadcasting alarm and alert information.

IV. RELATED WORK

The research of heterogeneous wireless sensor web is not new. In an application for habitat monitoring, Estrin et al. [1] proposed a system architecture in which data filtered by local processing on way through larger, more capable and more expensive nodes.
References [2] [3] provide other two examples of real sensor webs with heterogeneous nodes for processing and transport tasks. In above works, the necessity of heterogeneity and the mechanisms of packet forwarding and processing are demonstrated and described.
Sensing models are of two types. They are single sensing model and multi sensing model. Incursion finding process in these two models is explored by Wang et al. [4]. In his work, the combination of finding probability and web parameters such as transmission range, sensing range, and node density are considered for experiments under single sensing models.
Lee et al. [5] analyzed WSW in heterogeneous web environment under variouskinds of exploitation s for maximizing lifetime of web. Their studies revealed that life time of WSW can be maximized by using certain mechanisms and especially by adding micro servers that affect life time of web positively.
Xi Peng et al [6] proposed a security management model for self organizing wireless sensor webs based on incursion finding. It can prevent most of attacks. Then an analysis of

each layer of webs in security model is discussed and the security management measures in the data link layer and web layer are described in detail especially. Such a structure is built based on the existing encryption and authentication protocols.

Byunggil Lee et al., [7] have developed management platform and security framework for WSW. The proposed framework has advantages as regard secure association and incursion finding. This also provides the background a WSW, its security issues and requirements.

Zhang and Lee [8] are among the first to study the problem of incursion finding in wireless Ad-hoc

Webs Liu et al. [9] have explored the effects of sensor mobility on sensing coverage and finding capability in a mobile WSW. It is demonstrated that sensor mobility can improve the sensing coverage of the web, and provide fast finding of targeted events.

Wang et al. [10] have provided a unifying approach in relating the incursion finding probability with respect to the incursion distance and the web parameters (i.e., node density, sensing range and transmission range), under single-sensing finding and multiple-sensing finding models, in both homogeneous and heterogeneous WSWs.

Qi Wang et al., [11] have developed a intruder finding algorithm of low complexity for static wireless sensor web. The incursion finding model includes characteristics that determine the average frequency of execution of order. A distributed algorithm in which the sensor collects the information from the neighboring nodes to analyses the anomalies if any from the neighbors. The incursion finding algorithm on detecting anomalies packets received from its neighbours basic alarms to report the anomaly.

V. PURPOSED MODEL

Our objective is to detect all incursions in various WSW. In this section, we purposed single sensing model and multiple sensing finding model in heterogeneous WSW to detect intruder .The purposed system aims to manage available energy in efficient manner to enhance the web scalability, flexibility and lifetime. We divide sensor web into clusters which are again partitioned into sectors. It will minimize the energy consumption by avoiding all the nodes needing to send data to a distant sink node. It uses anomaly finding technique in such a way so that phantom incursion finding can be avoided logically.

A. Assumptions

A sensor can be in any one of the following states:

- New Member Suspected Malicious from a point of the web boundary, given an incursion distance D > 0, the corresponding incursion finding volume V is almost an oblong volume as shown in figure .3.
- GENUINE → DEAD ISOLATED
- Each sensor node has a unique id in the web.
- Each member node has authentic wake-up token.
- A protocol is used to assign a secure wakeup and sleep schedule for the sensor nodes.
- Sink node is honest gateway to another web.
- Sensor nodes excluding leaf nodes and forwarding sector heads in the system
- participate in incursion finding process.
- Generally, sector coordinator is responsible for anomaly finding and sector monitor is responsible for finding of incursion.
- Anomaly can be detected on the basis of energy consumption rate, allotted wakeup schedule, authentic wakeup token, number of packets received within a time interval. Reputation of sensor node needs to be considered during incursion finding.

VI. ALGORITHM-MODEL DIAGRAM

The algorithm for node selection trying to select the high capacity nodes compared to other one. High capacity means large sensing range and transmission range as shown in figure.2.

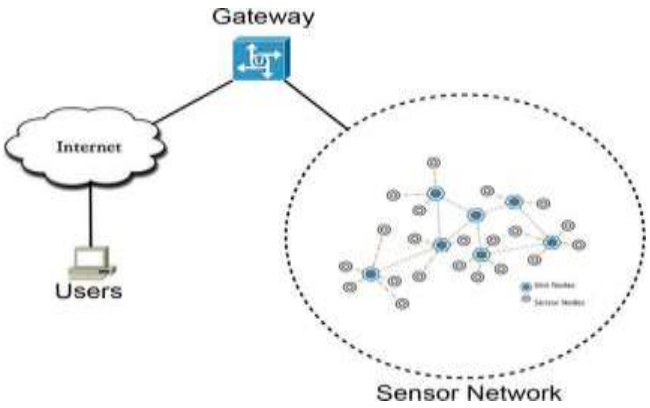

Figure 2: Proposed algorithm

A. Single-Sensing Finding

An intruder is detected when it enters the sensing range of a sensor. When the intruder enters the area through the boundary and the boundary is covered by the sensors, then the intruder will be detected as soon as it enters the WSW area. Otherwise, it has to move a certain distance D before detected by any of the sensors. When the intruder starts

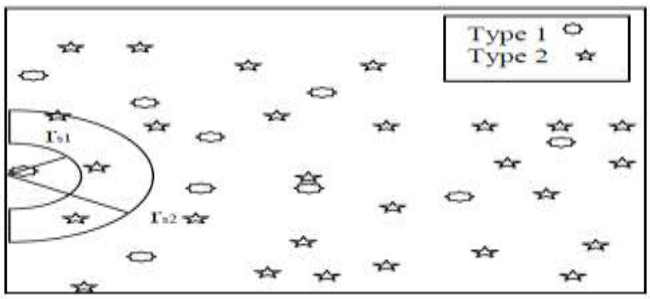

Figure 3: The area covered by sensors at the bound

Theorem 1

The probability P(D) that an intruder can be immediately detected once it enters a heterogeneous WSW can be given by,

$$p\,D = 0 = 1 - e^{-n1}$$
$$i=1$$

Where ni is the number of type i nodes activated in the area πrSi2/2.

Proof:

Here the area we need to consider when the intruder enters from the boundary is A1=(πrS12)/2, A2=(πrS22)/2,..AN =πrSN2/2 as shown in figure 1.So P(0, A1),(0,A2)….P(0,AN) gives the probability that there is no Type 1, Type 2…Type N sensors in that area. the probability that neither type 1 nor type 2….nor type N are given P(0,A1)P(0, A2)…..P(0.AN)=1-e-n1e-n2…e-nN where n1,n2,…nN are the number of selected nodes from each type. So the probability of detecting the intruder when it enters the boundary is given by complement P(0,A1)P(0,A2)….P(0,AN)=1-e-n1e-n2 ….e -nN.

Theorem 2

Suppose η is the maximal incursion distance allowable for a given application, the probability P (D) that the intruder can be detected within η in the given heterogeneous WSW can be derived as

$$p\,D < \eta = 1 - e^{-n1}\ i=1$$

Where ni is the number of sensors participating in incursion finding area Ai= 2ηrSi+(1/2) rSi2

Proof: This can be proved just like above theorem.

B. Multisensing

In the multi-sensing finding model, an intruder has to be sensed by at least m sensors for incursion finding in a WSW. The number of required sensors depends on specific applications. For example, at least three sensors' sensing information is required to determine the location of the intruder. Multi sensing in a heterogeneous WSW is explained in fig 2. Here multiple sensors have to detect a intruder at the same time.

Theorem 3

Let Pm (D= 0) be the probability that an intruder is detected immediately once it enters a WSW in multi sensing finding model. It has

$$Pm(D = 0) = 1 \quad P(i,Aj)$$
$$j=1\ i=0$$

Where Aj is the area covered by type j sensor and we are assuming that nj of type j sensors are activated in the area Aj.

Proof: This theorem can be proved just like above theorems. Here the area is only one half circles with radius rs.. P (i, A) gives the probability of detecting the intruder with i sensors.

$$P(i,Aj)\ i=0$$

gives the sum of the probabilities of detecting the intruder with less than m sensors. So the complement will give the multi sensing probability as shown in figure.4.

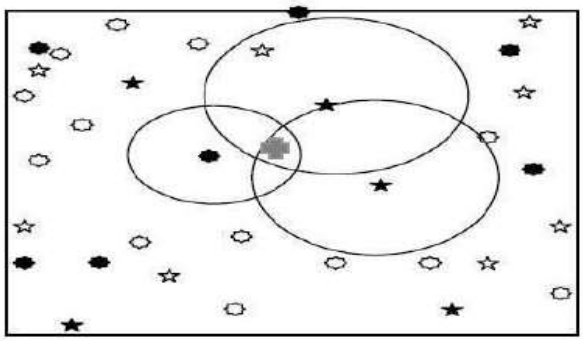

Figure 4: Multi-Sensing

VII. CONCLUSION

In this paper, we propose a novel solution to decide how many and where the heterogeneous nodes should be eployed in the randomly deployed sensor web. The imulation results show that our solution is practicable and useful to increase the web lifetime and reliability. It has been observed that these incursion finding systems are not adequate for protecting WSW from intruders efficiently. The need of the day is an IDS for detecting incursions accurately in an energy-efficient manner. Simulation proves the effectiveness of proposed model.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao,"Habitat monitoring: application driver for wireless communications technology," in Proc. ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, Costa Rica, April 2001

[2] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Webs for Habitat Monitoring," Intl. Workshop on Wireless Sensor Webs and Applications (WSWA '02), Atlanta, GA, Sept. 2002.

[3] H. Wang, D. Estrin, and L. Girod, "Preprocessing in a Tiered Sensor web for Habitat Monitoring," in Proc. of the IEEE Conf. on Acoustics, Speech, and Signal Processing, Hong Kong, China, April 2003 .

[4] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal,"Incursion finding in homogeneous and heterogeneous wireless sensor webs," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008..

[5] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Exploitation on Lifetime Sensing Coverage in Sensor Webs (IEEE SECON). (2004).

[6] Xi Peng, Wuhan Zheng Wu, Debao Xiao, Yang Yu," Study on Security Management Architecture for Sensor Web Based on Incursion Finding "' IEEE, Volume: 2,25-26 April 2009.

[7] Byunggil Lee, Seungjo Bae and Dong Won Han, "Design of web management platform and security frame work for WSW", IEEE International conference on signal image technology and internet based system, 2008.

[8] Y. Zhang and W. Lee. Incursion Finding in Wireless Ad-Hoc Webs. In Proc. ACM MobiCom, pages 275-283, 2000.

[9] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor webs," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Webing and Computing (MobiHoc), 2005.
[10] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal ,"Incursion finding in homogeneous and heterogeneous wireless sensor webs,"IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.
[11] Qi Wang, Shu Wang, "Applying an Incursion finding algorithm to wireless sensor webs", Second international workshop on Knowledge Discovery and Data Mining, 2009.