IJCSE International Journal of Computer Science and Engineering Open Access
Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

An Efficient Intruder Detection System against Sinkhole Attack in Wireless Sensor Networks: A Review

Rohit Aggarwal [1*] and Khushboo Bansal [2]

[1,2]Department of Computer Science and Engineering,
Desh Bhagat University, Punjab, India

www.ijcseonline.org

Received: Mar/28/2016 Revised: Apr/07/2016 Accepted: Apr/22/2016 Published: Apr/30/2016

Abstract: This Wireless sensor network is deal with sensing the information from deployed area. For data transmission from source node to destination node various routing protocols is used. Due to routing the energy consumption occurred in the network. In wireless sensor network energy consumption is one of the main problems because every node is operated by battery. In wireless sensor network energy utilization is one of the primary issues in light of the fact that each node is operated by battery. In wireless sensor networks, sensors expend energy both in detecting information and transmitting the detected information to a base station. The power utilization for transmitting information is an exponential function of the separation from the sensor to the base station. Power utilization for detecting information is controlled by the kind of sensor and in addition the routing protocol. The issue in this paper is to build the life time of the sensor systems. To have expansive system life time's everything nodes need to minimize their energy utilization.

Keywords: Wireless Sensor Networks, Applications of WSN, Routing in WSN, Intrusion Detection System, Sinkhole Attack

I. Introduction

1.1 Wireless Sensor Network: WSN networks compose possibly large number of wireless sensor nodes that are resource constrained in terms of energy, memory, computing capabilities and communication strange. A sensor node will be also referred to as just node or sensor in the sequel. There are various type of application of WSN are already present in health care, navigation, rescue, intelligent transportation, social networking, gaming application fields and critical infrastructure protection. This network is of tenant attended and deployed in harsh environments [4]. WSNs are hence subject to several threats because of their nature. Basically in this paper we focus on the security of the WSN. In particular, we cope with a fundamental, specific and dreadful security attack. Mobile WSNs are subject to the so-called clone attack. It consists in replicating and deploying the captured sensors to launch a variety of malicious activities. Replicating a node implies cloning the node ID and all the cryptographic material that is associated to that ID, as well as introducing further code to be executed this code supporting the adversary's goals [3,5]. The topology of the WSNs can change from a straightforward star system to a progressed multi-bounce remote lattice system. In WSNs, the main source of life for the nodes is the battery. Corresponding with different nodes or detecting exercises expends a considerable measure of energy in handling the information and transmitting the gathered information to the sink. As a rule (e.g. surveillance applications) it is undesirable to supplant the batteries that are exhausted or depleted of energy [2, 4].

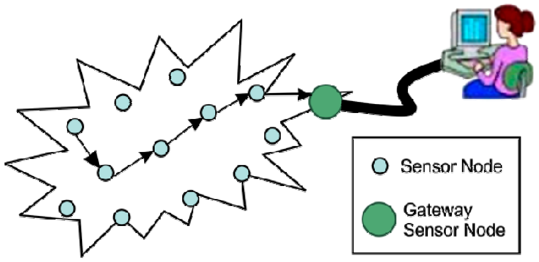


Figure 1: Wireless Sensor Network

1.2 Parts of WSN

1.2.1 Sensor Node: This is a centre part of WSN. This hub assumes different parts in WSN. For example straight forward sensing, information stockpiling, steering and information preparing [6].

1.2.2 Clusters: Clusters are the authoritative unit for WSNs. The thick way of these systems obliges the requirement for them to be separated into bunches to rearrange assignments such a correspondence [7].
1.2.3 Cluster heads: Cluster heads are the dealing with the bunch head. They frequently are expected to overseeing assignment in the bunch [8].
1.2.4 Base Station: The base station is at the upper level of the progressive WSN. It gives the correspondence connect between the sensor system and the end-client.
1.2.5 End User: The information in a sensor system can be utilized for an extensive variety of utilizations. Hence a specific application may make utilization of the system information over the web utilizing a PDA or even a desktop PC [9, 12].

1.3 Routing In WSN

In the wireless network nodes are distributed over the network and multiple nodes serve many messages. Each node used shared resource, so to transmit data from one node to another many decision has to be made, because of many path has been exist in the network to send data from source to destination [10, 11].

1.3.1 Routing Protocols in WSN

We can reduce the energy consumption by using various techniques like data aggregation, clustering and data-centric methods. The routing protocols can be classified as flat, hierarchical or location-based as follow:
1.3.1.1 Flat networks: In this network equal nodes are used. Hence each node plays the same role. This network has no logical hierarchy [14].
1.3.1.2 Hierarchical networks: The nodes are partitioned into a number of small groups called clusters.
1.3.1.3 Location-based networks: In location-based clustering the location of the sensor nodes plays an important role. Base station is used to send data to a particular location [13].

1.4 Applications of WSN

1.4.1 Area monitoring: Area monitoring is a typical use of WSNs. In Area monitoring the WSN is sent over a district where some wonder is to be observed. A military case is the utilization of sensors distinguishes foe interruption. A non-military personnel case is the geo-fencing of gas or oil pipelines [16].
1.4.2 Health care monitoring: The medical applications can be of two sorts i.e. wearable and implanted. Wearable gadgets are utilized on the body surface of a human or exactly at close closeness of the client. The implantable medical gadgets are those that are embedded inside human body.
1.4.3 Environmental/Earth sensing: There are numerous applications in monitoring environmental parameters. They share the additional difficulties of unforgiving situations and diminished power supply.
1.4.4 Air pollution monitoring: Wireless sensor networks have been conveyed in a few urban areas (Stockholm, London and Brisbane) to screen the centralization of hazardous gasses for natives.
1.4.5 Forest fire detection: A system of Sensor Nodes can be introduced in a forest to recognize when a flame has started begun [17, 18].

1.5 Intrusion Detection System

One of the key highlights of a WSN is its multihop distributed operations which include more intricacy as far as security attack recognition and prevention. In a multihop conveyed environment, it is extremely hard to find aggressors or malevolent hubs. Numerous security assault identification and prevention mechanism are intended for WSNs [1]. However a large portion of the current arrangements are fit for taking care of just a couple security assaults. Most secure routing protocols are intended to counter few security assaults. Additionally new media access systems are intended to handle concealed hub issue or childishness.
1.5.1Classes of IDSs: One is known as signature-based IDS where the marks of diverse security assaults are kept up in a database. This sort of IDS is viable against remarkable security assaults. On the other hand, new assaults are hard to be recognized as their marks would not be display in the database.
1.5.2 Signature-Based IDSs: Signature based IDS also called rule based IDS. System has predefined standards of diverse security attacks. At the point when the system's conduct demonstrates any deviation from the predefined rules, it is named as an attack. Signature based IDSs are appropriate for known interruptions; however they can't distinguish new security assaults or those assaults having no predefined rules [1].
1.5.3 Anomaly-Based IDSs: Anomaly based IDS screens system exercises and groups them as either typical or

noxious utilizing heuristic methodology. The vast majority of anomaly based IDSs distinguish interruptions utilizing edge values that is any action beneath a limit is ordinary while any condition over an edge is delegated an interruption [19].

1.5.4 Hybrid IDSs: Hybrid IDSs are a blend of both anomaly based and signature based approaches. Hybrid components as a rule contain two identification modules one module is dependable of recognizing remarkable assaults utilizing marks while the other is in charge of distinguishing and learning typical and malevolent examples or screen system conduct deviation from ordinary profile. Hybrid IDSs are more exact regarding assault location with less number of false positives.

1.5.5 Cross Layer IDSs: Cross layer outline is a generally new security method in which diverse parameters crosswise over OSI layers are traded for ideal arrangements. Traditional IDS works at a solitary layer of the OSI model and henceforth can screen and identify interruptions at that specific layer. For instance system layer Intrusion Detection System can distinguish just directing assaults however can't react to MAC, physical or transport layer irregularities [20].

1.6 Sinkhole Attack

In a sinkhole attack the foe's point is to draw almost all the movement from a specific zone through a bargained hub making an allegorical sinkhole with the enemy at the inside. Sinkhole attack regularly works by making a bargained node look particularly appealing to encompassing nodes as for the routing algorithm. Sinkhole attack is hard to counter in light of the fact that directing data supplied by a node is hard to check. As a case, a portable workstation class enemy has a solid force radio transmitter that permits it to give a transmitting so as to amaze course with enough energy to achieve a wide territory of the system. A traded off node pulls in all the movement from its neighbours by telling its neighbour that it has most limited route to reach to the base station. This route is simulated top notch route [15].

2. REVIEW OF LITERATURE

S. Misra, et al. [1] “Energy efficient learning solution for intrusion detection in Wireless Sensor Networks” The protocols in Wireless Sensor Networks (WSN) have a one of a kind necessity for being of low many-sided quality and vitality effective. Because of their conceivable arrangement in remote areas for common, instructive, experimental and military purposes, security which incorporates interruption location and interruption aversion is of most extreme significance. In this paper, we propose a basic, low intricacy and vitality mindful convention for interruption identification in WSN. The convention is learning toward oneself and appropriated in nature.

W. Dargie, et al. [2] "A consistent handover for WSN utilizing LMS channel" We propose a MAC convention that backings the portability of hubs in remote sensor systems. The convention empowers blast transmission and consistent handover to accomplish high throughput and to decrease bundle conveyance inactivity and parcel misfortune. A versatile channel constantly assesses the RSSI estimations of got affirmation bundles and chooses whether a portable hub ought to exchange a correspondence to a close-by hand-off hub with a superior connection quality. The handover process itself happens without breaking a current connection. This paper introduces the configuration, usage and assessment of the MAC convention.

J. Petajajarvi, et al. [3] "Delicate handover technique for portable remote sensor systems in view of 6LoWPAN" In numerous remote sensor system applications the sensor hubs needs to be versatile. Keeping in mind the end goal to help portability, the administration of a few issues, for example, steering, handover, security, tending to and auto-setup of the system needs to be taken care of. Previously, the principle center of sensor system examination has been on static sensor systems, consequently numerous portability related issues stay unsolved.

Qingtian Sun, et al. [4] "Vitality examination of sensor hubs in WSN taking into account discrete-time queuing model with a setup" Wireless sensor system is a vitality compelled framework. Vitality proficiency and information idleness are two essential execution measures expected to be considered when planning a remote sensor system. Taking the force administration mode in IEEE 802.15.4, considering into record the exchanging system from the slumber mode to the dynamic mode, a discrete-time queuing model with a setup is assembled, and the examination of the queuing model in enduring state is given.

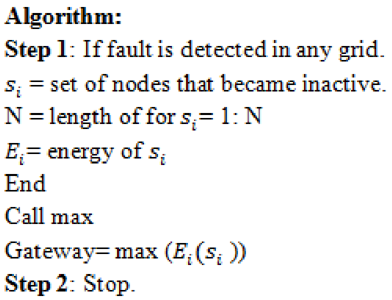
J.M.L.P. Caldeira, et al. [5] "Intra-portability handover improvement in social insurance remote sensor systems"

Health observing of patients is a typical assignment in human services houses from nursing homes to healing facilities. Restorative staff moves near to patients and gathers their observing body parameters. To help the general state control of observed patients, it could be performed in self-sufficient, continuous, and remotely way.

R. Silva, et al. [6] "another methodology for multi-sink situations in WSNs" Wireless sensors systems are ease systems constituted by unobtrusive gadgets with constrained assets, whose principle capacity is checking. Taking into account the low cost of these gadgets, it will be shoddy to convey a lot of hubs to screen a substantial region. Nonetheless, to give an effective specially appointed system utilizing these restricted gadgets, new and advanced calculations ought to be proposed. The vast majority of the current work about WSNs are in light of recreation studies and don't take in thought designing techniques.

3. APPROACHES USED

DFCA approach: In a distributed clustering algorithm for WSNs called DFCA (Distributed fault-tolerant clustering algorithm) is recommended that addresses both the issues, i.e. cluster arrangement in light of remaining energy of the entryways and adaptation to internal failure of the WSNs attributable to death of a few portals. In DFCA, the sensor nodes select legitimate CH by considering a cost capacity which comprises of remaining energy of the CH, the separation between sensor node to the CH and separation from the CH to the base station. In group development, DFCA takes think about the sensor nodes that have no CH inside of their correspondence range. DFCA additionally displays a conveyed run time recuperation of the broken group individuals because of sudden disappointment of the CH.



```
Algorithm:
Step 1: If fault is detected in any grid.
$s_i$ = set of nodes that became inactive.
N = length of for $s_i$= 1: N
$E_i$= energy of $s_i$
End
Call max
Gateway= max ($E_i(s_i)$)
Step 2: Stop.
```

Malicious detection approach: Sensor nodes in sensor systems are typically conveyed in unfriendly situations for example, war zones. Thus a sensor node might be traded off or out of capacity and afterward gives wrong data that might delude the entire system. This issue is called as the Byzantine problem. For instance, a traded off sensor node (noxious hub) can continually report inaccurate data to higher layers. The aggregator (FN or AP) in higher layer might make a wrong total result because of the impact of the malicious node. It is subsequently a critical issue in sensor networks to detect malicious nodes regardless of such Byzantine problem.

$$E = \sum_{n=1}^{N} W_n \times U_n$$

Where E is the aggregation result and is the weight ranging from 0 to 1. An essential concern is about the definition of sensor node's output. In practice, the output information may be “false” or “true” information or continues numbers such as temperature reading. Thus the definition of output is usually depending on the application where the sensor network is used.

Mac protocol: There are distinctive MAC protocols utilized as a part of the customary wireless network. MAC protocols utilized as a part of wired environment can't be utilized as a part of remote environment since crash happening at the collector is to be evaded. In wired network the sender distinguishes crash however since sign quality is for all intents and purposes the same all through the wired medium, this does not represent any huge issue. However in remote system the sign quality devalues in converse extent to the square of the separation agreeing Fries free space mathematical statement. An approach to make the MAC protocol energy efficient by addressing the problem of frame losses in cases where the communicating nodes are mobile in nature. Probability of error free reception of the frame as given in when using Manchester coding is

$$P_{efr} = (1 - BER)^{8f}(1 - BER)^{8(f-1)2.0}$$

Routing algorithm: Sink portability systems give a productive different option for parity energy utilization and delay the lifetime for WSNs. In many past routing algorithms or protocols for static sensor organizes, the directing tree is normally developed by building up express connections in the middle of source and destination sensor nodes. Source nodes more often than not transmit their checked information to their destination sensor node with single jump or multi-hop transmission way.

$$E_f = \frac{max(E(j)) - E(j)}{max(E(j))}$$

4. CONCLUSION

In wireless sensor network various malicious nodes has been introduced to perform various types of attacks on the network to degrade or collect same information. The new attack that has been used for acquiring information by performing sinkhole attack. Sink hole attack is performed on sink node attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data doesn't receive at base station that loss the information of the network. To overcome the issue of sink hole attack detection scheme has to be implement that detect attacking node and provide reliable information.

REFRENCES

[1] S. Misra, P.V. Krishna, K.I. Abraham "Energy efficient learning solution for intrusion detection in Wireless Sensor Networks" *Second International Conference on Communication Systems and Networks*, pp. 1-6, 2010.

[2] Satish Kumar, "A Study of Wireless Sensor Networks- A Review", *International Journal of Computer Sciences and Engineering*, Volume-04, Issue-03, Page No (23-27), Mar -2016.

[3] J. Petajajarvi, H. Karvonen "Soft handover method for mobile wireless sensor networks based on 6LoWPAN" *International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 2011, pp. 1 – 6, DOI: 10.1109/DCOSS.2011.5982208

[4] Qingtian Sun, Shunfu Jin, Chen Chen "Energy analysis of sensor nodes in WSN based on discrete-time queueing model with a setup" *Chinese Control and Decision Conference (CCDC)*, 2010, pp. 4114 – 4118, DOI: 10.1109/CCDC.2010.5498425.

[5] J.M.L.P. Caldeira, J.J.P.C. Rodrigues, P. Lorenz, L. Shu "Intra-mobility handover enhancement in healthcare wireless sensor networks" *14th International Conference one-Health Networking, Applications and Services (Healthcom)*, 2012, pp. 261 – 266.

[6] R. Silva, J. Sa Silva, M. Simek, F. Boavida "A new approach for multi-sink environments in WSNs" *International Symposium on Integrated Network Management*, 2009. IM '09. IFIP/IEEE, pp. 109 – 112.

[7] X. Chen, P. Yu "Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes" *IEEE 3rd International Conference on Biomedical Engineering and Informatics (BMEI)*, 2010, pp. 2863 – 2867.

[8] Yong-Sik Choi, Young-Jun Jeon, Sang-Hyun Park "A study on sensor nodes attestation protocol in a Wireless Sensor Network", *IEEE 12th International Conference on Advanced Communication Technology (ICACT)*, 2010, Volume: 1, pp. 574-579.

[9] S. Kwon, J. H. Ko, Jeong kyu Kim and Cheeha Kim, "Dynamic timeout for data aggregation in wireless sensor networks", *Elsevier Journal of Computer Networks*, 21 February 2011, pp. 650-664.

[10] R. L. Balla, V. Kotoju, "Sinkhole Attack Detection And Prevention in Manet & Improving The Performance of AODV Protocol", Compusoft, *An International Journal of Advanced Computer Technology*, 2013, PP 210-214.

[11] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated Coverage and Connectivity Configuration in Wireless Sensor Networks," *IEEE Conference on WSN, 2003*, pp 23-32.

[12] L. Doherty, K. S. J. Pister, and L. E. Ghaoui, "Convex Position Estimation in Wireless Sensor Networks," *International conference on INFOCOM, 2001*, pp 230-241.

[13] T. Dimitriou, I. Krontiris, T. Giannetsos and M. Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks", *In Algorithmic Aspects of Wireless Sensor Networks*, pp. 150-161.Springer Berlin Heidelberg, 2008.

[14] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An Efficient Intruder Detection Algorithm against Sinkhole Attacks in Wireless Sensor Networks," *Computer Communications, vol. 30*, pp. 2353-2364, 2007.

[15] Charanpreet Kaur and Amit Chhabra, "An Energy Efficient Multihop Routing Protocol for Wireless Sensor Networks", *International Journal of Computer Sciences and Engineering*, Volume-03, Issue-07, Page No (86-91), Jul -2015.

[16] Liping Teng, Yongping Zhang, "Sera: A Secure Routing Algorithm against Sinkhole Attacks For Mobile Wireless Sensor Networks", *Second International Conference on Computer Modeling and Simulation* 2010, PP 79-82.

[17] Nisarg Gandhewar, Rahila Patel, "Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", *Fourth International Conference on Computational Intelligence and Communication Networks,* 2012, PP 714-718.

[18] I. Krontiris, T. Dimitriou, F.C. "Freiling Towards intrusion detection in wireless sensor networks". In: Proceedings of the *13th European Wireless Conference, Paris, France* (April 2007).

[19] Gisung Kim, Younggoo Han, Sehun Kim, "A cooperative-sinkhole detection method for mobile ad hoc networks*",* *International Journal of Electronics and Communication 64* (2010) 390–397

[20] NS-2, The ns Manual (formally known as NS Documentation) available at following link:
http: //www. isi.edu/nsnam/ ns/do