ISSN: 0976-3104
SPECIAL ISSUE: COMPUTER SCIENCE

ARTICLE

OPTIMIZATION OF WATCHDOG SELECTION IN WIRELESS SENSOR NETWORKS

Praveen Kumar*, Shashank Joshi

Dept. of Computer Engineering, Bharti Vidyapeeth (Deemed to be University), College of Engineering, Pune, INDIA

ABSTRACT

Background: Wireless Sensor network (WSN) are broadly used today in various fields such as environmental control, surveillance task, object tracking, military applications etc. Guard dog is an observing strategy which distinguishes the getting rowdy hubs in the system. Watchdog method is a basic structure chunk to many belief systems that are intended for secure wireless antenna networks (WSNs). Advancing the guard dog procedures can spare vitality without giving up much and furthermore improve the security against specific assaults. **Methods:** This paper develops models that optimize the selection of watchdogs in WSNs. It focuses on two major facts: overlapping and coverage. Overlapping occurs when a sensor node is monitored by multiple watchdogs. It causes additional consumption of resources. It is inevitable due to the propagation characteristics of wireless signals. The full coverage occurs when each sensor node in a WSN is either monitored by at least one watchdog or working as a watchdog. **Results:** The presented models provide a better understanding of resource efficient watchdog deployment strategies. This paper presents KNN algorithm to optimize the watchdog selection for nodes. It will also detect the malicious activity of node in network.

INTRODUCTION

KEY WORDS
Watchdog, Wireless sensor network, Optimization model.

A remote sensor organize is an impromptu system which comprises of substantial number of little reasonable gadgets which are known as hubs (bits). These nodes are battery operated devices capable of communicating with each other without relying on any fixed infrastructure. The wireless sensor networks (WSNs) are often deployed in such an environment which is physically insecure and we can hardly prevent attackers from the physical access to these devices [1]. WSN comprises of base station alongside number of hubs that sense nature and send information to the base station. The base station (sink) is more intense than different hubs as far as vitality utilization and different parameters and fills in as an interface to the external world. The inner hubs sent in WSNs are the same as others, yet close to of nearby detecting they likewise give sending administration to different hubs. The interior hubs sent in WSNs are the same as others, yet next to of neighborhood detecting they additionally give sending administration to different hubs. A Wireless Sensor Network (WSN) is a particular remote system that is made out of various sensor hubs sent in a predefined zone for observing condition conditions such as temperature, pneumatic force, dampness, light, movement or vibration, and can speak with each other utilizing a remote radio gadget. WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility. Most sensor network protocols assume a high degree of trust between nodes in order to eliminate the overhead of authentication [2]. A watchdog organization is a technique of behavioral monitor of sensor nodes. In such a framework, various sensor hubs are chosen as guard dogs. It is considered as a powerful countermeasure to different assaults, for example, dissent of-benefit (DoS), sinkhole, and particular sending. Watchdogs are deployed to detect misbehaving nodes in a WSN. Each watchdog is responsible for its single hop neighbors [8]. It may overhear neighbors promiscuously or communicate with them for behavioral monitoring. It intermittently sends conduct reports to the base station (BS). It is likewise in charge of occasion driven detailing when irregularities are distinguished. As guard dogs are for the most part dedicated to the monitorial assignments, detecting activity lose assets. Ideal determination of guard dogs can diminish asset utilization in monitorial assignments [3].

Received: 14 May 2018
Accepted: 8 June 2018
Published: 11 June 2018

In [1] authors proposed an Intrusion Detection Systems (IDSs) that are proposed for WSNs is presented. Firstly, detailed information about IDSs is provided. Secondly, a brief survey of IDSs proposed for Mobile Ad-Hoc Networks (MANETs) is presented and applicability of those systems to WSNs is discussed. Thirdly, IDSs proposed for WSNs are presented.

In [2] authors first show that even if a watchdog can overhear all packet transmissions of a flow, any linear operation of the overheard packets cannot eliminate miss detection and is inefficient in terms of bandwidth. Also propose a lightweight misbehavior detection scheme which integrates the idea of watchdogs and error detection coding.

In [3] authors disclose the ineffective use of watchdog system in existing trust system, and thereby propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system's security in a sufficient level.

In [4] authors worked on Intrusion Detection Systems (IDS) in WSNs, and presents a comprehensive classification of various IDS to detect anomaly detection, misuse detection, and specification-based detection Protocols.

Our Objective

The Primary aim of this work is optimizing the watchdog node selection and in large area network it will check efficiently and send that node to particular cluster head and cluster head will be voluntarily make on the basis of sensor/battery status. And the communication will be more secured in the network and there is no any chance to interference of other any malicious node.

***Corresponding Author**
Email: praveendivine@gmail.com
Tel.: +91-9860690437

IIOAB JOURNAL
ISSN: 0976-3104

MATERIALS AND METHODS

Modules

Node
Cluster Head
Watchdog selection
Hacker

Node

A. Registration
- Node will register to the system, at the time of registration node will enter node name and password

B. Login

- If Node will provide correct nodename and password it will enter to the node account.
- Check the battery status of node if it status show comes near 30 % then it will go to cluster head one.
- If the battery status comes near 50% it will go to cluster head two.
- Which having battery status higher range among all node that one will be cluster head

Cluster head

- Cluster head chosen on the basis of battery status.
- Based on the KNN algorithm we will provide that node to particular cluster head.
- If cluster head two request file from cluster head one then the cluster head will send request to his entire node even the watchdog node.
- And if watchdog node has the file found then it will directly send that file to cluster node two .there is no need to communicate to cluster head one

Watchdog Selection

- Watchdog node will get resources or bandwidth to both of the cluster head.
- And that is the wastage of bandwidth in the large VPN network
- Detection of watchdog node and using KNN algorithm it will send to that cluster Head monitoring.

Hacker

- Hacker will login into the system.
- If the hacker will hack particular node then that node will not get file request and the status says this node has been hacked or compromised

There are two bunches on two unique pcs each group is having bunch head who is having most astounding weight among every one of the hubs in the bunch. The weight will be ascertained according to the piece battery of pcs. Making a two bunch according to the battery status like 10%-30% and 30%-100%. Here we need to get the covering hub in bunch.

Expect there are one group with 8 hubs on pc1 which is having the battery of 10-%30% and other second bunch with 8 hubs on pc2 having battery of 30%-100%.

Situation 1

In this if the main group is having 8 hubs and second bunch is likewise having 8 hubs on arrange. Hubs are having a similar battery reinforcement in both the bunches.

For instance, in the event that one bunch contains the hubs in arrange which is having the battery reinforcement of 10%-30% and second group is additionally having the battery reinforcement of 30%-100%. As of now the hubs which are having the battery of 25% however these hubs are likewise devours the vitality of both the bunch. Right now the Watchdog framework will evacuate the covering hubs in

ISSN: 0976-3104

organize by applying KNN calculation for ordering the hubs into a specific group. So it can expel the covering hubs into network [4].

Situation 2:

Any hub which is having most noteworthy bit battery reinforcement it will be pronounced as a Cluster head (CH) of that specific bunch.

Situation 3:

For instance, if CH1 hubs needs to speak with other CH2 hubs or send the information. At that point first hubs need to ask for the specific CH that he needs to send the information to CH2 hub. At that point CH1 ask for to CH2 that acknowledge the demand and get information.

PROPOSED ARCHITECTURE

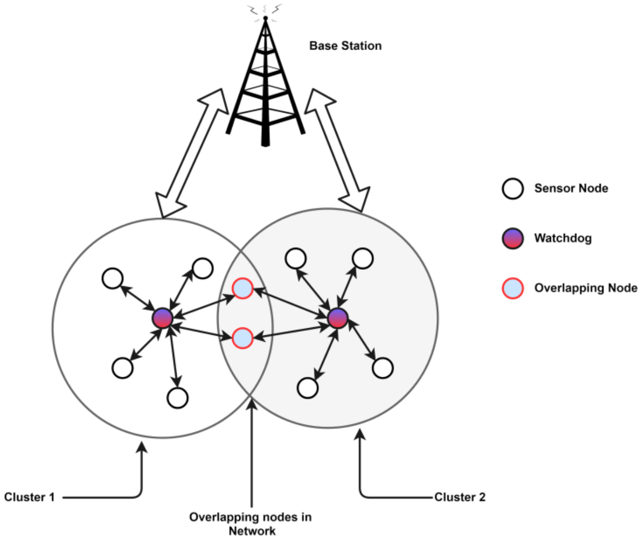

Fig. 1: System architecture

……………………………………………………………………………………

In this [Fig. 1] the exhibited models give a superior comprehension of asset effective guard dog sending procedures. This paper presents KNN algorithm to optimize the watchdog selection for nodes. It will likewise recognize the malevolent movement of hub in organizes.

Algorithm

The Blowfish Encryption Algorithm

Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc.Blowfish is a symmetric block encryption algorithm designed in consideration with

1. **Fast:** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
2. **Compact:** It can run in less than 5K of memory.
3. **Simple:** It uses addition, XOR, lookup table with 32-bit operands.
4. **Secure:** The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length.

It is suitable for applications where the key does not change often, like communication link or an automatic file encrypt.

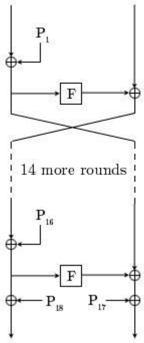

Fig. 2: The Feistel structure of blowfish.

Description of Algorithm

In [Fig .2] Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. This algorithm is divided into two parts.

1. Key-expansion
2. Data Encryption

Key-expansion

It will convert a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish uses large number of subkeys.These keys is generate earlier to any data encryption or decryption. The p-array consists of 18, 32-bit sub keys:

P1,P2,.............,P18

Four 32-bit S-Boxes consists of 256 entries each:
S1,0, S1,1,.......... S1,255
S2,0, S2,1,........... S2,255
S3,0, S3,1,........... S3,255
S4,0, S4,1,..............S4,255

Generating the Sub keys

The sub keys are computed utilizing the Blowfish calculation

1. Initialize first the P-exhibit and afterward the four S-boxes, all together, with a settled string. This string comprises of the hexadecimal digits of pi (less the underlying 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, and so forth.

2. XOR P1 with the initial 32 bits of the key, XOR P2 with the second 32-bits of the key, et cetera for all bits of the key (perhaps up to P14). More than once push through the key bits until the whole P-cluster has been XORed with key bits. (For each short key, there is no less than one identical longer key; for instance, if A will be a 64-bit key, at that point AA, AAA, and so on. are equal keys.)

3. Encrypt the every one of the zero string with the Blowfish calculation, utilizing the sub keys depicted in steps (1) and (2).

4. Replace P1 and P2 with the yield of step (3).

5. Encrypt the yield of step (3) utilizing the Blowfish calculation with the changed subkeys.

6. Replace P3 and P4 with the yield of step (5).

7. Continue the procedure, supplanting all passages of the P exhibit, and afterward every one of the four S-confines arrange, with the yield of the consistently changing Blowfish calculation.

Altogether, 521 emphases are required to produce all required sub keys. Applications can store the sub keys instead of execute this induction procedure various circumstances.

KNN algorithm

1. Determine parameter k = number of nearest neighbor.
2. Calculate the distance between the query instance and all the training samples.

3. Sort the distance and determine nearest neighbor based on th k th minimum distance.
4. Gather the category y of the nearest neighbor.
5. Use simple majority of the category of nearest neighbor as the prediction value of query instance.

Description of the algorithm

One of the least difficult and rather paltry classifiers is the Rote classifier, which remembers the whole preparing information and performs characterization just if the traits of the test protest coordinate one of the preparation illustrations precisely. An undeniable disadvantage of this approach is that numerous test records won't be grouped in light of the fact that they don't precisely coordinate any of the preparation records. A more refined approach, k-closest neighbor (kNN) order , finds a gathering of k protests in the preparation set that are nearest to the test question, and bases the task of a mark on the power of a specific class in this area. There are three key components of this approach: an arrangement of named objects, e.g., an arrangement of put away records, a separation or comparability metric to register removes amongst objects, and the estimation of k, the quantity of closest neighbors. To order an unlabeled question, the separation of this protest the marked articles is processed, its k-closest neighbors are recognized, and the class names of these closest neighbors are then used to decide the class name of the object. [Fig. 6] provides a high-level summary of the nearest-neighbor classification method. Given a training set *D* and a test object *x = (***x***_,y_)*, the algorithm computes the distance (or similarity) between *z* and all the training objects *(***x***, y) ∈D* to determine its nearest-neighbor list, *Dz*. (**x** is the data of a training object, while *y* is its class. Likewise, **x**_ is the data of the test object and *y_* is its class.) Once the nearest-neighbor list is obtained, the test object is classified based on themajority class of its nearest neighbors:
Majority Voting: *y_* = argmax*v* _ (**x***i ,yi)∈DzI (v = yi),* (18)

wherev*er* is a class label, *yi*is the class label for the *i*th nearest neighbors, and *I (·)* is an indicator function that returns the value 1 if its argument is true and 0 otherwise.

RESULTS

This project is better solution to finding the watchdog selection in network and with the use of this work in less resources or bandwidth uses we can optimize the selection of watchdog and communicate the network in secure way.

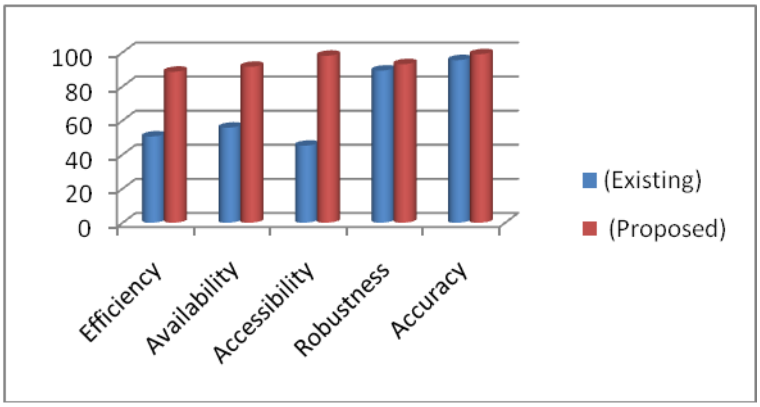

Fig. 3: Analysis graph

[Fig. 3] explains the pictorial representation of the table on the scale of 0 to 100 existing system and proposed system that is much more reliable in watchdog selection. easy to implement in the large network and accuracy of result done in lab network using of battery sensing in network and local area network it find very fast the watchdog area node and using the KNN algorithm whatever the battery sensing set to that cluser it will communicate and under that cluster head that node will work. if that node be with cluster head two somewhere and after finding the watchdog selection and it will send to cluster head 1 then it will efficiently communicate with cluster head two there is no any via connection with cluster head one.

compare the existing and proposed system in this proposed system result shows the selection of watchdog in large VPN network that need large setup and the accuracy and efficiency that is totally depends on the cluster head. Proposed system is much more robust and make reliable network and it is tested on several of our lab network implements the large node set with less resources Used achieve the robustness and accuracy of the watchdog area network node and send to the respective cluster head.

DISCUSSION

In the old system it was tedious find and optimizes watchdog selection in wireless network in large area network and with using of fewer resources it will send to the respective cluster head using KNN and using Blowfish encryption algorithm we are encrypt the network sending file.

Existing system

The factual basic leadership structure approach broadens our prior work in where a heuristic probabilistic directing calculation was proposed to upgrade the protection for the goal hub. It generally trade off client's security. Three basic ways to deal with alleviate examination endeavors are to: (I) change the physical appearance of every bundle at each bounce by means of jump by-bounce encryptions (ii) present transmission delays at each jump to de-relate movement streams, or (iii) acquaint sham activity with jumble activity designs. The initial two methodologies may not be attractive for minimal effort or battery-fueled remote systems, e.g., remote sensor arranges as (I) the ease hubs will most likely be unable to bear the cost of utilizing the computationally costly encryptions at each jump, and (ii) presenting delays at the transitional hubs may not be successful when there is little activity in the system. In this manner, we utilize the spurious movement way to deal with give protection by bringing down the enemy's recognition rates in a remote system. In particular, we consider a foe that uses the ideal most extreme a-posteriori (MAP) estimation strategy [5].

Disadvantages of existing system

1. Cannot detect collective attacks in diverse large scale networks.
2. The existing scheme cannot work reasonably balance privacy and data utility.

PROPOSED SYSTEM

It is a checking method which recognizes the getting into mischief hubs in the system. Guard dog procedure is a crucial building piece to numerous trust frameworks that are intended for securing remote sensor systems (WSNs). Improving the guard dog systems can spare vitality without giving up much and furthermore upgrade the security against specific assaults. This paper creates models that improve the choice of guard dogs in WSNs. It bases on two significant substances: covering and degree. Covering happens when a sensor center point is seen by various monitor mutts. It causes extra utilization of assets. It is unavoidable due to the causing characteristics of remote signs. The full extension happens when each sensor center point in a WSN is either checked by no short of what one monitor canine or filling in as a watch dog [6].

Advantages of proposed system

1. It cannot compromises users privacy.
2. It provides proper the transmission in network.
3. Optimize the watchdog selection for nodes.

CONCLUSION

We designed Watchdog system which is a monitoring technique and which detects the misbehaving nodes in the network. Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Optimizing the watchdog techniques can save energy without sacrificing much and also enhance the protection against certain attacks. Using blowfish encryption algorithm for data file sending within the network To optimize this we have used the KNN algorithm.KNN algorithm used in various pattern in this research work it will find the better and secure way to find the cluster head for node.

CONTRIBUTION

Detection of watchdog is the main scenario of proposed system. Finding the watchdog and separate to dedicated cluster head by using KNN algorithm. And it will good at large range VPN network and by this so much bandwidth and resources can be saved.

CONFLICT OF INTEREST

None

ACKNOWLEDGEMENTS

The authors would like to thank Prof. T. Charles Clancy and the anonymous reviewers for their careful review and helpful comments in this paper.

FINANCIAL DISCLOSURE

None

IIOAB JOURNAL ISSN: 0976-3104

REFERENCES

[1] M Batty, K Axhausen, et al. [2012] Smart cities of the future, European Physical Journal, Special Topics 214 : 481-518.

[2] I Butun I, S Morgera, R Sankar. [2014] A survey of intrusion detection systems in wireless sensor networks, IEEE Comm. Surveys and Tutorials, 16(1): 266-282.

[3] G Liang, R Agarwal, N Vaidya. [2010] When watchdog meets coding, in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010.

[4] P Zhou, S Jiang, et al. [2015] Toward energy efficient trust system through watchdog optimization for WSNs, IEEE Trans. on Information Forensics and Security, 10(3): 613-625.

[5] A Abduvaliyev, AK Pathan, et al. [2013] On the vital areas of intrusion detection systems in wireless sensor networks, IEEE Comm. Surveys and Tutorials, 15(3):1223-1237.

[6] Y Ren, VI Zadorozhny, et al. [2014] A novel approach to trust management in unattended wireless sensor networks," IEEE Trans. on Mobile Computing, 13(7): 1409-1423.

[7] J Duan, D Yang, et al. [2014] An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications, IEEE IoT Journal, 1(1): 58-69.

[8] Q Monnet, Y Hammal, et al. [2015] Fair election of monitoring nodes in WSNs," in Proc. IEEE ICC, June 2015, London, UK, pp. 1-6.

[9] J Hwang, T He, Y Kim. [2010] Exploring in-situ sensing irregularity in wireless sensor networks, IEEE Trans. on Parallel and Distributed Systems, 21(4): 547-561.

[10] Q Monnet, Y Hammal, et al. [2015] Fair election of monitoring nodes in WSNs, in Proc. IEEE ICC, London, UK, pp. 1-6.

[11] J Hwang, T He, Y Kim. [2010] Exploring in-situ sensing irregularity in wireless sensor networks, IEEE Trans. on Parallel and Distributed Systems, 21(4): 547-561.