A SURVEY ON MALICIOUS NODE RECOGNITION IN WIRELESS SENSOR NETWORK

P. Poornima[1]
Research Scholar,
Dept of Computer Science,
School of Computing Sciences,
VISTAS,
Pallavaram.

Dr.M.S.Nidhya[2]
Assistant Professor,
Dept of Computer Science,
School of Computing Sciences,
VISTAS,
Pallavaram.

Dr.R.Jayakarthik[3]
Associate Professor,
Department of Computer Science,
School of Computing Sciences,
VISTAS
Pallavaram.
Pallavaram

Abstract

Wireless Sensor Network is collection of sensor nodes, which is scattered in an environment. Sensor monitors the environment and sends information to sink node. End user can access the sink node. Malicious node in a network can corrupt a message and send to sink node. Then end user can take wrong decision based on corrupted message. Malicious node in a network can change the message as a corrupted message or misroute the packet or drop a packet. Hence a wrong message can be received by a user. It leads to drastic problem. To eliminate malicious node from a WSN, there are number of algorithms are proposed. In this paper, we analyzed number algorithms to detect malicious node in WSN.

Keywords: malicious node, wireless sensor network, detection algorithm, sink node.

1. INTRODUCTION

Wireless sensor networks (WSNs) are commonly collected the big quantity of sensor nodes having owning competencies of green statistics acquisition and capabilities sensing. They are attracting masses hobby from a couple of fields for his or her brilliant prospects. In real software situations, distinct range of localization schemes typically suffer from one in every of kind attacks. In range-based totally schemes, earlier than distribution information [1].

Maintaining a routing route that could offer an excessive achievement rate of facts transmissions is one of the most important requirements for dependable statistics transmissions in industrial WSNs. If the routing path in use research a high form of packet drops, it isn't always probable that the facts packets may be delivered to the sink node on time. This demands short identification of the terrible normal performance of the routing direction. Once the routing course is confirmed to be poorly acting, it has to get replaced with an opportunity one. The identification and alternative of the poor routing path require suitable routing metrics and course update strategies. For the update processes, a prolonged period for routing metric evaluation will result in an extraordinary boom in the community reaction time. Then again, diminishing the assessment span will decrease the network reaction time yet it will also present more prominent overhead. A blame hub on account of low vitality or diverse thought processes has a lower sending power than ordinary hubs, so the likelihood of adequately sending messages to its ensuing jump hub can be decline than that of any regular hub. The sending charge of a malignant hub in a specific sending attack is decline than an ordinary hub in shiny new because of its horrible parcel losing [2].

An immoderate stage of cooperation is vital for applications that require actual-time information transmission, such as soldiers relaying facts in a battlefield. However, the limited electricity supply of cellular gadgets raises doubts about the capacity of every node to be fully cooperative. As a result, packet delivery can't be assured even if malicious nodes aren't present, and resending information packets does no longer provide a tremendous solution [3].

However, the limited strength deliver of cell gadgets will increase doubts approximately the capability of every node to be certainly cooperative. As a result, packet delivery cannot be confident even supposing malicious nodes are not gift, and resending statistics packets does now not provide a exceptional solution. If malicious nodes are observed in a MANET, they'll attempt to reduce community connectivity (and thereby undermine the network's security) by way of pretending to be cooperative but in impact losing any information they'll be intended to pass on. These moves may additionally result in defragmented networks, far flung nodes, and appreciably reduced network average performance. Thus, the fast development in measurements exchange, by utilizing the utilization of the joining and combination of WSN/IoT requires a constant improvement of new time of stop to-stop hub server security calculations providing unnecessary phase of wellbeing that can be demonstrated by method for a radical resistance to cryptanalysis [4].

The present day-day consider is a continuation of this examination by method for way of affirming the Wireless sensor systems, because of their temperament, are more in danger of insurance dangers than explicit systems. Improvements in WSNs have brought around the production of numerous conventions particularly advanced for insurance capacities. A large portion of these conventions are not green in expressions of setting an extreme computational and control consumption trouble on little hubs in WSNs.

2. RELATED WORKS

Amjad Mehmood et al., [5] prescribe a realities based setting mindful strategy for managing the interruptions produced by utilizing pernicious hubs. The contraption works on skill base, set at the base station; it really is utilized to hold the exercises created by utilizing the hubs in the system. The events are named and the group heads (CHs) are said to dam perniciously rehashed games exercises produced. The CHs additionally can get instructive measurements roughly the malevolence of interloper hubs by methods for utilizing the utilization of their induction motors. The system of games logging and examination by utilizing the base station significantly impacts
the execution of hubs in the network by utilizing way of bringing down the more prominent insurance related burden on them. The base station plays different highlights on the put away events got a magnificent method to diminish the heap at the CH and the scope of powerful occasions. Excess occasions and individuals which have been coming about because of a couple of system conditions and no longer by method for the utilization of interlopers are wiped out by methods for method for the base station.

Zhihua Zhang et al., [6] proposed an interruption recognition dependent on powerful U.S.A . Setting and various leveled be given as valid inside WSNs is proposed, that is adaptable and appropriate for persistently changing WSNs described by utilizing method for changes inside the perceptual environment, advances of conditions of hubs, and varieties in remember charge. A multidimensional - level various leveled be given as genuine with system inside the level of sensor hubs (SNs) and bunch heads (CHs) contemplating intelligent remember, genuineness consider, and content material texture concur with is advanced, which consolidates direct assessment and comments based absolutely assessment inside the settled bounce go.

Zoubir Hamici et al., [7] proposed the keys time method is one part of the cryptographic quality of a lot of approaches. The gadget begins off advanced by changing over the passphrase linked to the records framework salt, with a hash calculation; explicitly a SHA-256bits.

Kemedi Moara-Nkwe et al., [8] proposed a one of a kind key innovation plot that takes increase of both the vitality and simplicity of conventional slip-ups revising codes and furthermore the assorted variety of recurrence channels accessible on 802.15.Four consistent hubs to produce keys from got flag vitality readings. The privateness enhancement organize fills basic needs,

1) to guarantee perfect ahead and in reverse insurance and
2) to ensure that the absolute last key has bits that are legitimately dispensed and to procure

this reason, the protection intensification arrange plans the essential component in one of these way that a most recent session key administrative work a hash chain that makes utilization of each the former key and the hashed expense of the front line substantial layer produced key as contentions.

Van Nhan Vo et al., [9] proposed a model and advancement plot that makes utilization of a remotely fueled quality jammer to upgrade mystery in EH-WSNs. The considered vitality collecting Wi-Fi sensor systems EH-WSN display incorporates a few power stations, numerous SNs (sources) and their base station, a decent jammer, and two or three latent busybodies. We isolate the variant into extents:

1) The power stations exchange RF vitality to the supply SNs and
2) The convey SNs transmit data to their base station,

even as a wonderful jammer produces sticking signs towards more than one spy. Utilizing factual inclinations of the sign-to-clamor proportion, the shut shape articulations of the presence shot of the mystery usefulness and mystery blackout danger are determined.

Zhao Zhang et al., [10] proposed to amplify the life of hindrance protection, those obstruction covers should be planned to avoid a security bother, name rupture. In a heterogeneous Wi-Fi sensor arrange, given a lot of obstruction covers each with a lifetime, we test the problem of finding an entire life-expanding subset with a break loosened rest wake up planning.

3. RESULT ANALYSIS

TABLE 1.1 Comparison of various malicious node detection algorithms

S. No	Algorithm	Description	Merits	Demerits
1.	**Breach-Free Scheduling**	The most extreme lifetime rupture free calendar issue, one need to discover a subset of obstruction spreads to frame a break free timetable.	• First come first serve is pretty simple and easy to implement. • Eventually, every process will get a chance to run, so starvation doesn't occur.	• Time consuming

2.	**Genetic Cryptography Algorithm**	The material procedures of choice, mating, and change are portrayed. Choice is an arbitrary procedure which is one-sided so the chromosomes with higher wellness esteems are bound to be chosen.	• It can find ***fit*** solutions in a very less time. • The random mutation guarantees to some extent that we see a wide range of solution.	• It is really hard for people to come up with a good heuristic which actually reflects what we want the algorithm to do. • It might not find the most optimal solution to the defined problem in all cases.
3.	**Pseudo code for Randomness Sharing Stage**	Pseudo Random Number Generator (PRNG) alludes to a calculation that utilizes numerical equations to deliver arrangements of arbitrary numbers. PRNGs produce a grouping of numbers approximating the properties of irregular numbers.	• Easy to understand • Useful in data exploration • Less data cleaning required.	• Over fitting. • Not fit for continuous variable
4.	**Localization algorithm**	The limitation calculation does not have to appraise the channel gain h I , as the calculation fuses the channel measurements for estimation.	• Often it is easy to translate pseudocode into a programming language, a step which can be accomplished by less experienced.	• The main disadvantage are that it does not provide a visual representation of the programming
5.	**Maximum-match filtering (MMF) algorithm**	The Spectrum Sensing Data Falsification (SSDF) assault is a kind of DOS assault where the aggressors change the range detecting report to propel the base station to take a wrong synergistic choice with respect to the empty range band in different systems. In this paper, we have proposed the	• The calculation can't segregate between the essential flag and clamor, and thus makes it hard to set the limit utilized for essential client identification, particularly at low SNR.	• The Matched Filter Technique is very important in communication as it is an good filtering technique which maximizes the signal to noise ratio (SNR).

		Maximum-Match Filtering calculation (MMF) for cooperative range detecting and range basic leadership in CWSNs, which is executed at the base station to counter the SSDF assault.		
6.	**Flow Splitting Optimization Algorithm**	Disconnected improvement apparatuses possess the advantage of energy for dull calculation, though SCOOT must work rapidly as it reacts to traffic distinguished in the city.	• Produce system with a longer effective operational system. • Produce more flexible system.	• Require more extensive and accurate. • May be difficult to customize.
7.	**Data Aggregation Algorithms.**	An information collection conspire is vitality proficient on the off chance that it amplifies the usefulness of the system. System lifetime, information exactness, and dormancy are a portion of the huge execution proportions of information collection calculations.	• With the help of data aggregation process we can enhance the robustness and accuracy of information which is obtained by entire network.	• The cluster head means data aggregator nodes send fuse these data to the base station .this cluster head or aggregator node may be attacked by malicious attacker.
8.	**Opportunistic routing**	pioneering steering is intended for the transmission from the source to the goal by multi-hub cooperation in the sending way. For all the forwarders, the goal is extraordinary. There are two issues in the planar structure arrange by utilizing the hypothesis of deft directing for communicate information spread.	• Robust capable of dealing with disturbances. • Suitable for convergent materials flow.	• Excessive planned needed • More sensitive to disturbances

9.	**Malicious Node Detection Algorithm**	The natural qualities of remote sensor systems, for example, confinement of hub vitality, storage room and registering limit and unattended in the outside, arrange hubs are effectively caught by the adversary, malignant hubs exist inside the system effectively.	• Can adopt to the changing network conditions .	• Overhead increases with mobility of nodes.
10.	**Cumulative sum (Cu Sum) Algorithm**	CUSUM examination was utilized for checking change in fracture adequacy, and we tried regardless of whether adequate careful results were accomplished.	• Code get complicated when lot of conditions are required.	• State transition is easy to think. • Code is easy and less complicated.

In this tabular column we compare various algorithms which detects malicious node

The table1.1 shows the comparisons of different algorithm. The Genetic Cryptography Algorithm is more efficient and user friendly. The process is faster in timer when comparing with other systems. The detection method complexity is reduced in the method.

4. CONCLUSION

The paper discuss about the survey on detection of malicious node. Through this paper, the given and define of the current researches associated with numerous techniques and techniques of malicious detection. The different algorithm and the malicious detection process key points advantage and disadvantage were discussed throughout the paper. Based on the review the Genetic Cryptography Algorithm is more efficient in the detection of malicious modes. In future the network can be extended to the Bayesian network model to predict the malicious nodes in advance.

References

[1]. Xingcheng Liu, Senior Member, IEEE, Shaohua Su, Feng Han, Yitong Liu, Zhihong Pan," A Range-Based Secure Localization Algorithm for Wireless Sensor Networks", IEEE Sensors Journal ,doi 10.1109/JSEN.2018.2877306.

[2]. Hongjun Dai, Yu Liu, Fenghua Guo and Zhiping Jia," A Malicious Node Detection Algorithm Based on Principle of Maximum Entropy in WSNs", Journal Of Networks, Vol. 7, NO. 9, September 2012, doi:10.4304/jnw.7.9.1376-1383.

[3]. Van Nhan Vo 1, Tri Gia Nguyen 2, (Member, Ieee), Chakchai So-In 1, (Senior Member, Ieee), Zubair Ahmed Baig3, And Surasak Sanguanpong 4," Secrecy Outage Performance Analysis For Energy Harvesting Sensor Networks With A Jammer Using Relay Selection Strategy", Special Section On Security And Trusted Computing For Industrial Internet Of Things, *Digital Object Identifier 10.1109/Access.2018.2829485*.

[4]. Amjad Mehmood1, Akbar Khanan2,3, Muhammad Muneer Umar4, Salwani Abdullah2, Khairul Akram Zainol Ariffin2, And Houbing Song 5, (Senior Member, IEEE),” Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks”, special section on security analytics and intelligence for cyber physical systems, *Digital Object Identifier 10.1109/Access.2017.2770020.*

[5]. Zhihua Zhangi, Hongliang Zhui, Shoushan Luo1, Yang Xin1, And Xiaoming Liu2,” Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks”, *Digital Object Identifier 10.1109/Access.2017.2717387.*

[6]. Idris Abubakar Umari, Zurina Mohd Hanapi1, (Member, Ieee), A. Sali2, (Member, Ieee), Zuriati A. Zulkarnaini, (Member, Ieee),” TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks “,*Digital Object Identifier 10.1109/Access.2017.2672827*

[7]. Zoubir Hamici, *Senior Member, Ieee,”* Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways”, Ieee Journal of Biomedical and Health Informatics, Doi 10.1109/JBHI.2018.2860980.

[8]. Kemedi Moara-Nkwe 1, Qi Shi1, Gyu Myoung Lee1, And Mahmoud Hashem Eiza2,” A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks”, *Digital Object Identifier 10.1109/Access.2018.2806423.*

[9]. Van Nhan Vo 1, Tri Gia Nguyen 2, (Member, Ieee), Chakchai So-In 1, (Senior Member, Ieee), And Dac-Binh Ha3,” Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer”, *Digital Object Identifier 10.1109/Access.2017.2768443.*

[10]. Zhao Zhang , *Member, Ieee,* Weili Wu, *Senior Member, Ieee,* Jing Yuan, and Ding-Zhu Du,” Breach-Free Sleep-Wake up Scheduling for Barrier Coverage With Heterogeneous Wireless Sensors”, Ieee/Acm Transactions On Networking, Digital Object Identifier 10.1109/TNET.2018.2867156.

[11]. Zhihua Zhang1, Hongliang Zhu1, Shoushan Luo1, Yang Xin1, And Xiaoming Liu2,” Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks”, *Digital Object Identifier 10.1109/Access.2017.2717387.*

[12]. Idris Abubakar Umar1, Zurina Mohd Hanapi1, (Member, Ieee), A. Sali2, (Member, IEEE), Zurati A. Zulkarnain1, (Member, Ieee),” TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks “,*Digital Object Identifier 10.1109/Access.2017.2672827.*

[13]. Zoubir Hamici, *Senior Member, Ieee,”* Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways”, Ieee Journal of Biomedical and Health Informatics, Doi 10.1109/JBHI.2018.2860980.

[14]. Kemedi Moara-Nkwe 1, Qi Shi1, Gyu Myoung Lee1, And Mahmoud Hashem Eiza2,” A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks”, *Digital Object Identifier 10.1109/ACCESS.2018.2806423.*

[15]. Zhao Zhang , *Member, Ieee,* Weili Wu, *Senior Member, Ieee,* Jing Yuan, and Ding-Zhu Du,” Breach-Free Sleep-Wake up Scheduling for Barrier Coverage With Heterogeneous Wireless Sensors”, Ieee/Acm Transactions On Networking, Digital Object Identifier 10.1109/TNET.2018.2867156.

[16]. By Ruixin Niu , *Senior Member Ieee,* Aditya Vempaty, *Member Ieee,* and Pra mod K. Var shney, *Life Fellow Ieee,”* Received-Signal-Strength- Based Localization in Wireless Sensor Networks”, Digital Object Identifier: 10.1109/JPROC.2018.2828858.

[17]. *Pinaki Sankar Chatterjee1, Monideepa Roy1,”* Lightweight cloned- node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs”, *IET Wirel. Sens. Syst.*, 2018, Vol. 8 Iss. 3, pp. 121-128.

[18]. Xiaoyang Lai1 And Huan Wang2,” Rnob: Receiver Negotiation Opportunity Broadcast Protocol for Trustworthy Data Dissemination in Wireless Sensor Networks”, *Digital Object Identifier 10.1109/Access.2018.2871082.*

[19]. Guozhi Li, Songtao Guo, *Member, Ieee,* Yang Yang and Yuanyuan Yang, *Fellow, Ieee,”* Traffic Load Minimization in Software Defined Wireless Sensor Networks”, Ieee Internet of Things Journal, Doi 10.1109/JIOT.2018.2797906.

[20]. Anes Yessembayev, Dilip Sarkar, *Senior Member, Ieee,* and Faisal Sikder, *Member, Ieee,”* Detection of Good and Bad Sensor-Nodes in Presence of Malicious Attacks, and Its Application to Data Aggregation”, Doi10.1109/TSIPN.2018.2790164, Ieee Transactions on Signal and Information Processing over Networks, Doi 10.1109/TSIPN.2018.2790164.

[21]. Xingcheng Liu, Senior Member, IEEE, Shaohua Su, Feng Han, Yitong Liu, Zhihong Pan,” A Range-Based Secure Localization Algorithm for Wireless Sensor Networks”, , Ieee Sensors Journal, Doi 10.1109/JSEN.2018.2877306.

[22]. Xiaoqiang Ren?, Karl H. Johanssony, Dawei Shiz and Ling Shi,” Quickest Change Detection in Adaptive Censoring Sensor Networks”, Ieee Transactions on Control of Network Systems, Doi 10.1109/TCNS.2016.2598250.