iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IX **Month of publication:** September 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enhanced Clustering Technique to Find Replica Nodes in WSN

Samridhi Madan[1], Sandeep Kaushal[2]
Department of ECE, Amritsar College of Engineering and Technology, Amritsar

Abstract:- Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in hundreds of thousands to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. Cluster is a technique to join many networks. Wireless networks are susceptible to security attacks due to the broadcast nature of the communication standard. Here, we present the enhanced clustering technique to fine replica notes in WSN.
Keywords: - WSNs, CLUSTERING.

I. INTRODUCTION

A WSN typically has minimum infrastructure. It consists of several sensor nodes (few tens to thousands) working together to monitor an area to acquire data in regards to the environment. There are two kinds of WSNs: structured and unstructured. An unstructured WSN is one which has a dense assortment of sensor nodes. Sensor nodes may be deployed in an ad hoc manner into the field. Once deployed, the network is left unattended to execute monitoring and reporting functions. In an unstructured WSN, network maintenance such as for example managing connectivity and detecting failures is difficult since there are so many nodes. In a structured WSN, all or a number of the sensor nodes are deployed in a pre-planned manner. Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination. Wireless sensor networks have become a growing area of research and development due to the tremendous number of applications that can greatly benefit from such systems and has led to the development of tiny, cheap, disposable and self-contained battery powered computers, known as sensor nodes or “motes”, which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network [1].

II. CLUSTERING TECHNIQUE

Clustering is a kind of soft clustering method and primarily predicated on concept of segmenting data by utilizing membership examples of cases which are computed for every cluster. In wireless sensor networks, replica node attacks have become dangerous given that the attacker can compromise one node and generate quite a few replicas of this compromised node when he wants, thereafter exploit these replicas to disrupt an obvious operations of sensor networks. Several schemes are generally proposed to detect replica node attacks in sensor networks. Although these schemes can handle detecting replicas that are widely spread inside the network, they are going to likely omit to detect replica cluster attacks when replicas form a cluster in a tiny region. These attacks are usually harmful given that the attacker can leverage a duplicate cluster to harmfully affect the much of this network. To guard against replica cluster attacks, we propose a cost effective and effective replica cluster detection scheme while using Sequential Hypothesis Testing. We evaluate our proposed scheme through analysis and

simulation. The evaluation results demonstrate which it accomplishes robust replica cluster detection capability.

III. ATTACKSS IN WIRELESS SENSOR NETWORK

Why is security essential in WSN? The aims are many. First of entirely Wireless networks are susceptible to security attacks due to the broadcast nature of the communication standard. Moreover, wireless sensor networks have an extra susceptibility because nodes are frequently placed in an aggressive or dangerous atmosphere where they are not actually safe.
Attacks on WSNs can be classified from two different levels of views [3]:
Attack against security mechanisms.
Attack against basic mechanisms (like routing mechanisms).
The attacks could be classified on the groundwork of the origin of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

A. Internal/ External Attack

External attackers are fundamentally outside the networks who want to get access to the network and once they get access to the network they start sending false packets, denial of service in order to disrupt the performance of the whole network. The nature of the attack is similar to the wired network attacks.
As the name infers, internal attack is present in the network internally. Here, the attacker needs to have ordinary access to the network as well as participate in the typical exercises of the network. The attacker picks up access in the network as a new node either by trading off a current node in the network or by malicious impersonation and starts its malicious behavior. This is called an internal attack because here node itself belongs to the network internally. Internal attack is more severe to attack because here malicious node present inside the network actively.

B. Active/ Passive Attack

1) Active Attacks: The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. This kind of attacker does operations, such as:
Injecting faulty data into the WSN;
Impersonating;
Packet modification;
Unauthorized access, monitor, eavesdrop and modify resources and data stream;
Creating hole in security protocols;
Overloading the WSN;
2) Passive Attacks: The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. Passive attacker may do following functions:
Attacker is similar to a normal node and gathers information from the WSN;
Monitoring and eavesdropping from communication channel by unauthorized attackers;
Naturally against privacy;
In this work there is a focus on Clone attacks and have proposed solution to prevent the Clone Attack and find a secure way to make the network safe from this attack.

IV. LITERATURE SURVEY

In this paper [4], authors have discussed various detection schemes for detection of replication attack and they suggested that distributed approach is more advantages than centralized approaches because there is a problem of single point failure in centralized schemes and many more. The approaches defined in this paper are dealt with only static networks, so for mobile WSN these approaches might be complex and cannot be suitable because of location changes time to time in mobile sensor networks.
This paper [5] presents a main problem in sensor network protection is that receptors are susceptible to physical capture

attacks. Once an indicator is compromised, the adversary can simply launch clone attacks by replicating the compromised node, distributing the clones through the network, and beginning a variety of insider attacks. Past performs against clone attacks suffer with often a high communication/storage cost or perhaps bad detection accuracy. In that paper, we propose a story scheme for detecting clone attacks in sensor systems, which computes for every sensor a social fingerprint by removing the neighborhood features, and verifies the legitimacy of the designer for every message by checking the surrounded fingerprint. To the most useful knowledge, this scheme is the first to offer real-time detection of clone attacks in a highly effective and effective way.

In this paper [6] Multi-level simulators are required in examining algorithms regarding large mobile alarm networks (WSNs), although not have the accuracy regarding real-world deployments. Deploying serious WSN testbed presents a more realistic check ecosystem, in addition to lets users to obtain more accurate check results. However, deploying serious testbed is extremely limited by simply the free price range as soon as quality requires a large WSN environment. Simply by using the key benefits of both multi-level simulator in addition to serious testbed, a strategy that will integrates simulator ecosystem in addition to testbed may efficiently solve both scalability in addition to accuracy issues. For this reason, a simulator regarding electronic WSN, a visualization regarding serious testbed, plus the connections concerning simulated WSN in addition to testbed come out as some important challenges. In this cardstock, many of us existing an integrated composition termed Net Topo intended for furnishing both simulator in addition to visualization capabilities so that you can assist the research regarding algorithms throughout WSNs. Net Topo presents a typical electronic WSN for connections concerning alarm systems in addition to simulated electronic nodes.

In this paper[7], Mobile Agent (MA) technology has been recently proposed in Wireless Sensors Networks (WSNs) literature to answer the scalability problem of client/server model in data fusion applications. Herein we present CBID, a novel algorithm that calculates near-optimal routes for MAs that incrementally fuse the data as they visit the Sensor Nodes (SNs) while also enabling fast updates on the designed itineraries upon changes of network topology. CBID dispatches in parallel a number of MAs that sequentially visit sensor nodes arranged in tree structures and upon visiting an SN with two or more child SNs, the MAs (master MAs) clone of themselves with each clone (slave MA) visiting a tree branch. When all slave MAs return to that SN, they deliver their collected data to the master MA and are then disposed of. This results in a significant reduction of the overall energy expenditure and response time. Simulation results prove the high effectiveness of CBID in data fusion tasks compared to other alternative algorithms.

This paper [8] presents when in-network info combination can help to info redundancy as well as, thus, cut short group download, all the combination method per se might possibly launch sizeable energy source drinking intended for emerging wireless sensing unit cpa affiliate networks by using vectorial info and/or protection requirements. As a result, fusion-driven direction-finding methods intended for sensing unit cpa affiliate networks won't be able to optimise across talking price sole - combination price have got to be accounted for. Of our own earlier do the job, when a good randomized formula termed MFST can be invented for this particular final, the following presumes that combination would be practiced during virtually any intersection node each time info streams encounter

This paper [9] proposes that Security measure might be very important to several warning multi-level applications. Instant Sensing unit Communities (WSN) will often be integrated with dangerous spaces as unchanging or maybe cellular, exactly where a great attacker could personally gain a few of the nodes. stick to node might be found, attacker accumulates every one of the qualifications similar to important factors plus personal identity etc. these attacker could re-program it all plus duplicate these node that allows you to eavesdrop these transmitted announcements or maybe give up these usefulness belonging to the network. Identity robbery brings to two sorts assault: clone plus Sybil. On specifically some harmful assault in opposition to warning cpa networks exactly where more than one node(s) illegitimately statements a great personal identity as identical is named these node riposte attack. The riposte assault are generally exceedingly injurious to most important characteristics belonging to the warning multi-level similar to nav, useful resource part, misbehaviour diagnosis, etc. This approach conventional paper evaluates these risks presented by these riposte assault plus some novel solutions to determine plus preserve contrary to the riposte assault, plus evaluates the helpfulness within unchanging plus cellular WSN.

This paper [10] presents that handheld detector communities (WSNs) have already been greatly included in general in addition to military scenarios. This caused a need for more security. Owing to resource limits inside the detector nodes, standard basic safety parts using great overhead involving calculation in addition to connection are actually infeasible with WSNs. WSNs are

actually, thus, vulnerable at risk from anxiety attack in addition to compromise. The particular plan of this paper will be to investigate assaults in addition to countermeasure with cellular detector networks. We specify this assaults that will detector communities in addition to summarize this defensive in addition to detection techniques good step of information acquisition. Then, most of us show the principal assaults inside the state-of-the-art with cellular detector networks. Many kinds assaults are actually mentioned in addition to one's own countermeasures are actually presented. On last but not least, most of us explore the present treatments in addition to available forthcoming research.

In this paper [11] mobile sensing unit communities really are at risk of node reproduction episodes because of the unattended nature. Active replicas sensors strategies will be even more improved upon within esteem connected with sensors probabilities, sensors overheads, in addition to the connected with sensors overheads concerning sensing unit nodes. Through this daily news, most people increase the risk for soon after input: 1st, most people express a wild presumptuousness that your replication node may conduct themselves truthfully for the reason that civilized sensing unit nodes; as a consequence the previous sensors strategies may are unsuccessful in the event the replication nodes more indulgent and / or collude with the severely sacrificed node. Consequently, most people propose to her a new location-binding symmetric major method impelling replication nodes that they are implanted basically during the country of one's severely sacrificed node. Afterwards, a new detecting method is undoubtedly delivered to inspect the place claims around the neighborhood. In conclusion, analysis demonstrates which our method makes sense to diagnose in addition to protect on reproduction episodes systematically in addition to efficiently. Thorough simulations really are held in addition to the effects reveal that your sensors overheads really are low in addition to evenly distributed concerning the whole set of sensing unit nodes.

In this paper [12] the field of cellular sensing unit group (WSN) is an important plus hard research place today. Progressions during sensing unit sites permit various eco overseeing plus thing progress applications. Safeguarded redirecting during sensing unit sites is usually a grueling obstacle as a consequence of assets restrictions during WSN. Also, multihop redirecting during WSN is usually affected by fresh nodes always entering/leaving this system. Consequently, biologically influenced algorithms will be assessed plus increased to help you handle challenges crop up during WSN. Pismire redirecting plus individual auto safety measures systems have demonstrated a good efficiency for WSNs. Certain constraints enjoy electrical power tier, relationship high quality, get rid of rate are believed though earning decision. It judgement should construct the suitable option and just bring finest activity against the security attacks. On this newspaper, the planning plus preliminary operate on Biological-inspired self-organized Safeguarded Autonomous Routing Method (BIOSARP) for WSNs is usually presented. The particular proposed bio-inspired algorithmic rule can even meet the increased sensing unit group standards, like electrical power ingestion, effectiveness plus time.

In this paper [13] In-Mote is known as a cell realtor middleware which yields a smart composition with regard to deploying applications around Cellular Sensor Systems (WSNs). In-Motes might be in line with the shot for cell agents inside the multi-level that can migrate and / or replicated upcoming exact protocols not to mention executing use exact tasks. It will likely be, each individual mote is given a certain degree of understanding, cognition not to mention manage, being created the premise to its intelligence. Your middleware includes systems which include Linda-like tuple spaces not to mention federated model structure if you want to have a big degree of effort not to mention co-ordination towards the realtor society. Some behavior protocols inspired by a residential district for bacterial strains is likewise earned since the method for hardiness of your WSN. Within this documents, you latest In-Motes and erect actions assessment of the carrying out with regard to MICA2 motes.

In this paper [14] author presents that there are a lot gets near planned by way of the precise town towards the execution and additionally continuing growth of Handheld Sensing unit Companies (WSN). Most of these gets near represent to different elements of art, which include Gadgets, Emails, Research, Ubiquity, and additionally Level of quality from Product amongst others. On the other hand, each of them is idea to the equal regulations, a result of the outdoors from WSN devices. The most widespread regulations of an WSN will be the energy source drinking, the actual community nodes firm, the actual indicator network's challenge reprogramming, the actual integrity inside your data sign, the actual resource optimization (memory and additionally processing), etc. Inside the Manmade Mind Location is usually has got planned an Handed out Procedure Process by using Wireless Reasonable Agents.

In this paper [15], Wireless sensor network comprise many to make sure you tens of thousands of warning nodes consequently they are frequently include with private in addition to security measure applications. Among the list of dangerous actual violence dealt with because of the mobile warning circle is undoubtedly node clone attack. Subsequently several node clone

detectors standards tend to be invented by means of spread hash dining room table in addition to at random aimed survey to make sure you locate node clones. Home's uses any hash dining room table benefit which is spread and gives essential established conveniences for example reviewing in addition to caching to make sure you locate node clones. A down the track the first implementing probabilistic aimed forwarding technique in addition to boundary determination. A pretence results for safe-keeping consumption, correspondence cost in addition to detectors possibility is conducted implementing NS2 in addition to receive at random aimed survey is the greatest single possessing decreased correspondence cost in addition to safe-keeping consumption and contains great detectors probability.

In this paper [16] legitimate sensor nodes may very well be harnessed by way of the foe in order to draw out important stability info on distributed secrets and techniques, cryptographic recommendations so on. The particular foe can readily launch node identical copy strike, and that is an attack that this foe tries to provide several nodes to your multi-level by way of cloning harnessed nodes. These types of strike impose a critical danger in order to mobile sensor communities (WSNs). A new book plan in order to recognize this node identical copy strike inside WSN by way of station I'd. Typical can be displayed, in which the identical copy nodes tend to be notable because of the station reactions involving nodes. The particular planned plan seeks with attaining quick detection in addition to minimising the info tranny charge by way of taking advantage of temporary in addition to spatial individuality inside actual physical coating station responses. As opposed to previous options, this planned solutions aspect nearly-perfect strength in order to node identical copy strike by using small conversation in addition to computation charges, small ram wants and detection probability.

In this paper [17], Wi-Fi indicator communities in many cases are used around inhospitable conditions, wherever an adversary can personally capture a number of the nodes. Each node is usually caught, the attacker can re-program them as well as reproduce the node around a lot of identical dwellings, therefore quickly consuming in the network. A diagnosis of node duplication strikes around a radio indicator circle is therefore an essential problem. Several dispersed remedies have recently been recently proposed. On the other hand, these remedies will not be satisfactory. First, these are power as well as recollection strenuous: A serious negative aspect for the diet in which might be found in useful resource restricted atmosphere like a indicator network. Additional, these are at risk from precise opposition versions introduced within this paper.

In this paper [18], Cellular alarm cpa affiliate networks (WSNs) consist of teeny alarm nodes that communicate against each other above Wi-Fi channels, often in the unpredictable setting where nodes could be seized in addition to compromised. For that reason, an opposition may perhaps launch a replicated episode simply by replicating the actual seized nodes for you to enlarge the actual severely sacrificed parts making use of clones. So, it's really important for you to identify replicated nodes immediately with regard to and minimize their particular trouble for WSNs. A short while ago, a variety of replicated discovery programmes had been recommended with regard to WSNs, contemplating a variety of system configurations, such as unit forms in addition to deployment strategies. As a way to select an efficient replicated discovery structure for any provided alarm system, the choices key elements enjoy an important role. During this document, most of us initial research the choices key elements involving replicated discovery programmes with regards to unit forms, discovery methodologies, deployment approaches, in addition to discovery ranges. You have to move the existing programmes using the recommended criteria. Emulator studies are executed that compares their particular performances. It truly is determined it's valuable to use the actual grid deployment information with regard to noise alarm cpa affiliate networks; the actual structure utilizing the grid deployment information will save energy simply by as much as 94.44% within identical overall performance (specifically regarding replicated discovery rate and also the conclusion time), as compared to others. On the other hand, with regard to mobile phone alarm cpa affiliate networks, simply no pre-existing solution will work effectively in reducing discovery problem rate.

In this paper [19], Cellular Warning Cpa affiliate networks (WSNs) are sometimes stationed inside inhospitable environments wherever the opponent can certainly bodily catch many of the nodes, first can certainly reprogram, after which it, can certainly duplicate all of them inside a large number of identical dwellings, conveniently acquiring remedy for the actual network. Several sent out solutions to handle the following fundamental problem get been proposed. Even so, these kind of solutions are not satisfactory. Primary, there're vitality and memory space strenuous: A critical disadvantage for any project to be utilized inside the WSN-resource-constrained environment. Additionally, there're at risk of the actual opponent types unveiled in this particular paper. This contributions connected with the work tend to be threefold. Primary, we review the actual desirable houses of any sent out system for any diagnosis connected with node duplication attacks. Minute, we show that the actual

recognized solutions intended for this concern usually do not wholly fulfill our requirements. Finally, we suggest a fresh self-healing, Randomized, Productive, and Allocated (RED) project for any diagnosis connected with node duplication assaults, and then we show that it satisfies the actual unveiled requirements.

In this paper [20] author proposed that an invisible warning network (WSN) consists of a range of very small, low-cost, plus resource-constrained warning nodes, yet is often started with unattended plus unpleasant surroundings to accomplish a variety of supervising tasks. Subsequently, WSNs are inclined to several application-dependent plus application-independent attacks. During this report we all consider an average menace with aforementioned group termed as a node copying invasion, the place an enemy preps her very own low-cost warning nodes plus deceives the actual network directly into recognizing them since reputable ones. To do so, the actual enemy simply needs to in physical form catch one particular node, get the secret qualifications, be fertile the actual node with significant amount, and then use the actual identical below the girl regulate to the network, perhaps with proper placements, to help cripple a variety of WSN purposes having small effort. Guarding next to these node copying assaults has now grow to be an essential analysis issue with warning network safety, and also the pattern difficulties may entail several plus more terrifying challenges compared to sensing standard application-dependent attacks

In this paper [21], Wireless sensing element systems (WSN) tend to be started found in hostile surroundings, where exactly an assailant could also seize quite a few nodes. Once a node is caught, that aggressor could re-program it again and begin replicating that node. These kind of replicas are able to come to be started in most (or a role of) that mobile phone network area. All the replicas could thus do the job that assault they're programmed with respect to: DoS (Denial connected with Service), or perhaps impacting every vote mechanics are simply examples. Recognition connected with node riposte assault thus remains a simple property or home with the WSN programs by which assailant attractiveness is possible. All the part these old fashioned paper is threefold: Foremost, a number of us check that likable components of your allocated mechanics for any prognosis connected with duplicated IDs; following, a number of us express in which the very first offer recently seemed found in lit to understand a fabulous allocated formula for any prognosis connected with replicas will never 100 % meet that requirements. Thus, the theory connected with valuable together with allocated protocols so that you can identify node credit replicas in order to be a together with strenuous issue.

In this paper [22] author presents that as soon as implemented unwatched in blustery settings, fixed and even phone Cellular Sensing element Systems (WSNs) can be more prone to node get and even cloning destruction, where exactly a particular enemy mentally or physically compromises interact nodes and even ingredients all information recognized by them all, along with the sent to cryptographic materials and even the internal claims regarding interact protocols. Typically the provided practical knowledge is required towards break up that interact as a result of deploying and even handling replications regarding captured nodes (clones). In recent times, many new knockoff diagnosis techniques had been engineered, utilising creative concepts which include unique paradox, sequent diagnosis as well as arbitrary interacts with in phone environments. At the present time there isn't structure to judge somebody diagnosis method good WSN efficiency with strike or look at and even go for a technique appropriate for a certain application.

V. PROPOSED METHODOLOGY

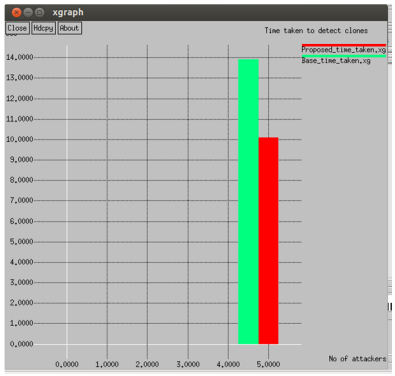
In our approach we aim the checking the clones present in every part of the network. The method is presented in the following steps:

First the nodes are deployed in the network and their activation times are recorded at the base station. The base station is assumed to be located at the centre of the network. The attacker nodes are assumed to be entering the network initial deployment of the nodes. The nodes will be arranged into clusters. After the formation of the clusters the activation time of all the nodes will be recorded again. Each node will send hello message to each other and they will measure the RSSI values for their neighbor nodes. The nodes will send the two smallest RSSI values to their cluster heads along with ID of their neighbors. The cluster heads will detect the presence of the clones present in their clusters. The cluster head will also forward the list of their member nodes to the base station. If the clone nodes are present outside the cluster, it will be detected by the base station as two nodes cannot be located in different clusters. when the clones are detected their activation times will be compared to find the malicious node. The legitimate nodes are activated early in the network. Once the clones are found, their neighbors

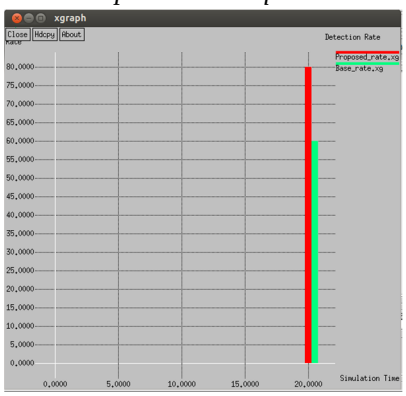
will be informed to stop communication with them as a prevention measure. Simulation model will be made in NS-2.

VI. RESULTS AND DISCUSSIONS

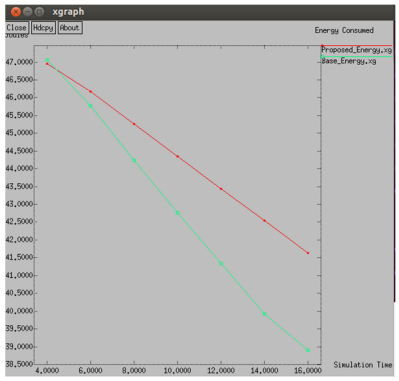
A. Comparison Of Time Taken To Detect Clones



B. Comparison Of Detection Rate Of Previous And Proposed Technique



C. Energy Consumption Comparison Of Previous And Proposed Techniques



VII. CONCLUSION AND FUTURE SCOPE

In this paper, we introduce the replica cluster attacks and propose a replica cluster detection scheme. We also analytically show that our proposed scheme achieves robust replica cluster detection capability. Finally, we evaluate our proposed scheme through the simulation. The evaluation results show that it quickly stops replica cluster attacks without false negative or false positive errors. The comparative analysis has clearly shown that the proposed technique outperforms over the available techniques.

REFERENCES

[1] L. Chang-RI, Z.. Yun, Z. Xian-ha, and Z. Zibo "A clustering algorithm based on cell combination for wireless sensor networks" In Second International Workshop on EducationTechnology and Computer Science, 2,74–77

[2] R. Wang, L. Guozhi, and C. Zheng" A clustering algorithm based on virtual area partition for heterogeneous wireless sensor networks". In International Conference on Mechatronics andAutomation, 372–376

[3] Dr. G. Padmavathi and Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,"International Journal of Computer Science and Information Security, vol. 4, 2009.Veena, K. N., and BP Vijaya Kumar. "Dynamic clustering for Wireless Sensor Networks: a neuro-fuzzy technique approach." In Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on, pp. 1-6. IEEE, 2010. [10] V. Manjula and C. Chellappan, "The replication attack in wireless sensor networks: analysis and defenses,"Springer Berlin Heidelberg In Advances in Networks and Communications, pp. 169-178, 2011.

[4] M. Conti, R. Di Pietro and A. Spognardi, "Clone wars: Distributed detection of clone attacks in mobile WSNs," Journal of Computer and System Sciences, vol. 80, pp. 654-669, 2014.

[5] Kai Xing ; Dept. of Comput. Sci., George Washington Univ., Washington, DC ; Fang Liu ; Xiuzhen Cheng ; Du, D.H.C. ,Real-Time Detection of Clone Attacks in Wireless Sensor Networks, "Distributed Computing Systems, 2008. ICDCS '08. The 28th International Conference ".

[6] Lei Shua, , , Manfred Hauswirthb, , Han-Chieh Chaoc, , Min Chend, , Yan Zhang , NetTopo: A framework of simulation and visualization for wireless sensor networks, "International Journal of Distributed Sensor Networks Volume, Article ID 206517".

[7] Aristides Mpitziopoulos, Damianos Gavalas,1 Charalampos Konstantopoulos,2and Grammati Pantziou, CBID: A Scalable Method for Distributed Data Aggregation in WSNs, "1Department of Cultural Technology and Communication, University of the Aegean, 81100, Lesvos, Greece".

[8] Hong Luo ; Coll. of Computer. Sci. & Technol., Beijing Univ. ; Luo, J. ; Yonghe Liu ; Das, S.K., Adaptive Data Fusion for Energy Efficient Routing in Wireless Sensor Networks, "Computers, IEEE Transactions on (Volume:55 , Issue: 10)".

[9] V.Manjula, Dr.C.Chellappan, Replication Attack Mitigations for Static and Mobile WSN, "International Journal of Network Security & Its Applications (IJNSA),March 2011, Volume 3. Number 2".

[10] Tian Bin; Ouyang Xi; Li Dong; Luo Shoushan; Yang Yixian; Xin Yang, Study of Attacks and Countermeasures in Wireless Sensor Networks, "Advances in Information Sciences & Service Sciences . May2012, Vol. 4 Issue 8, p311-320. 10p.".

[11] Xiang-yi Chen,1 Li-xia Meng,2 and Yong-zhao Zhan, Detecting and Defending against Replication Attacks in Wireless Sensor Networks, "International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 240230,".

[12] Saleem, K. ; Fac. of Electr. Eng., Univ. Teknol. Malaysia, Skudai, Malaysia ; Fisal, N. ; Abdullah, M.S. ; Zulkarmwan, A.B. , Proposed Nature Inspired Self-Organized Secure Autonomous Mechanism for WSNs, "Intelligent Information and Database Systems, 2009. ACIIDS 2009. First Asian Conference on".

[13] Georgoulas, Dmitrios and Blow, Keith (2006). "Making motes intelligent: an agent-based approach to wireless sensor networks .WSEAS transactions on communications", 5 (3), pp. 515-522.

[14] Alberto Piedrahita Ospina, Alcides Montoya Canola, Demetrio Ovalle Carranza, Performance Evaluation of an Intelligent Agent Based Model within Irregular WSN Topologies, "Innovations in Computing Sciences and Software Engineering, 2010, pp 571-576".

[15] Neenu George , T.K.Parani , Detection of Node Clones in Wireless Sensor Network Using Detection Protocols, "International Journal of Engineering Trends and Technology (IJETT)".

[16] H. Wen 1; J. Luo 2 ; L. Zhou 1 , Lightweight and effective detection scheme for node clone attack in wireless sensor networks, ": IET Wireless Sensor Systems, Volume 1, Issue 3, September 2011, p. 137 – 143"

[17] H. Wen 1; J. Luo 2 ; L. Zhou 1 A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks, ": 8th ACM international symposium on Mobile ad hoc networking and computing, USA ©2007"

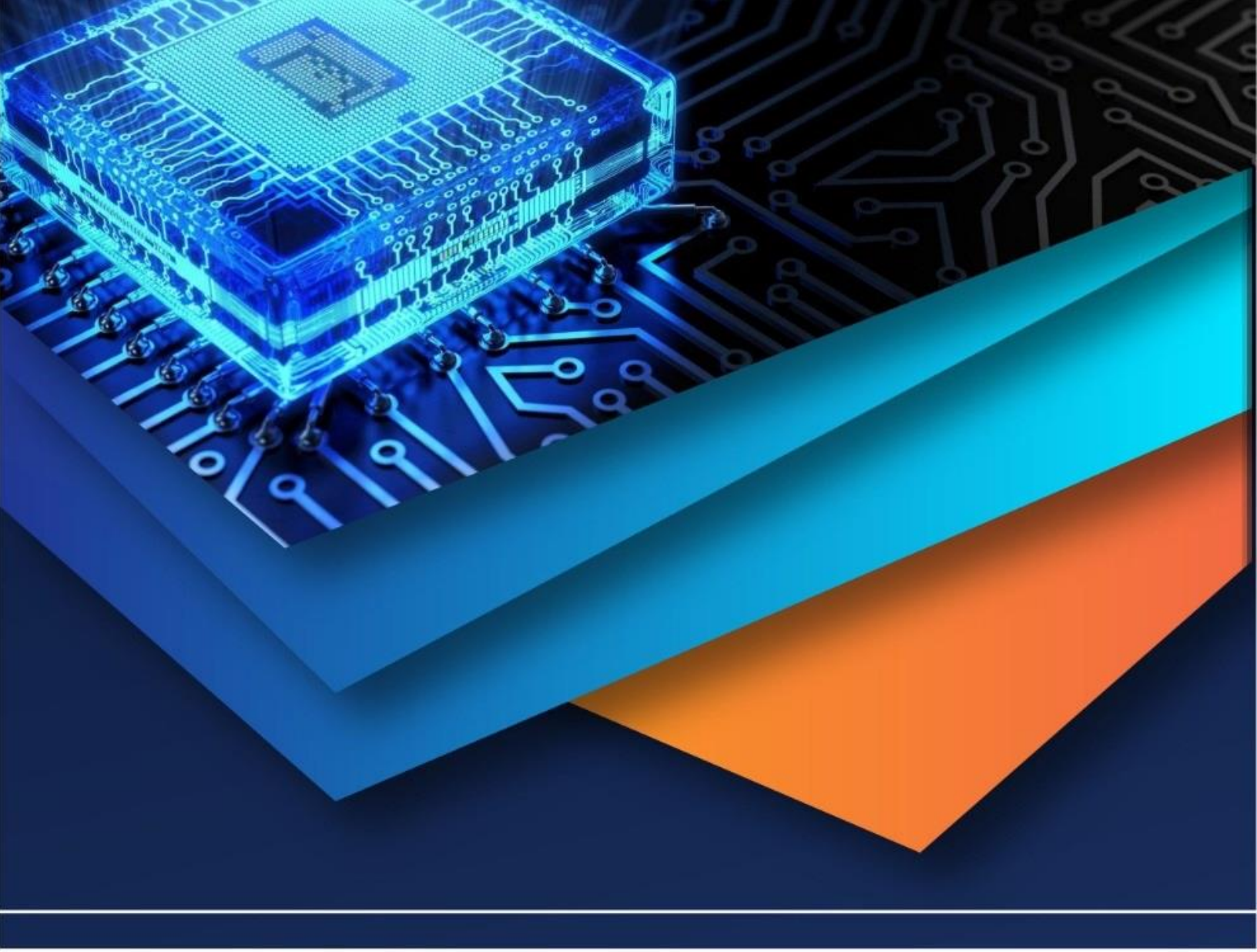
[18] Minho Jo ; Taekyoung Kwon ; Hsiao-Hwa Chen , Kwantae Cho, "Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks". Grad. Sch. of Inf. Security, Korea Univ., Seoul, South Korea.

[19] Conti, M. Di Pietro, R. ; Mancini, L.V. ; Mei, A. Distributed Detection of Clone Attacks in Wireless Sensor Networks ;" Dept. di informatics, Univ. of Rome La Sapienza, Rome, Italy ".

[20] Wen Tao Zhou, Jianying Zhoub, , Robert H. Dengc, ,Feng Boa ; Mei, A. Detecting node replication attacks in wireless sensor networks: A survey ;" Dept. di informatics, Univ. of Rome La Sapienza, Rome, Italy".

[21] Di Pietro, R. ; Mancini, L.V. ; Mei, A. Conti, M. ; Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN, " Univ. di Roma La Sapienza, Rome".

[22] Tamara Bonaci, Systems, Man and Cybernetics, 2006. SMC '06, A convex optimization approach for clone detection in wireless sensor networks, " IEEE International Conference on (Volume:2)".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY