Establishing self-healing and error correction in wireless sensor networks using honeypot database

V.Nagaraju 1, B.R.TapasBapu 2, M.Ramesh 3, S.K.Rajesh Kanna 4, P Sailaja 5

1 Professor, Dept of ECE, Rajalakshmi Institute of Technology, India
2 Professor, Dept of ECE, S.A. Engineering College, India
3 Assistant Professor, Dept of ECE, Saveetha School of Engineering, India
4 Professor, Dept of Mechanical, Rajalakshmi Institute of Technology, India
5 Assistant Professor, Dept of IT, Velammal institute of technology, India
vankadarinagaraju@ritchennai.edu.in

Abstract. The quantity of noxious assault has been ascending due to rise of fresh susceptibilities as well as types of assaults that has been found every day. The stemming of growing counts of pernicious movement in remote system, it has been of a great interest for assault examination as well as the recognizable proof of new dangers. In a model of this kind, safety has not been considered as a condition, but rather a procedure, that implies so as one have to continually enhance and improve safety instruments to ensure worms in system. In order to establish legitimate safety framework one has to recognize and examine the dangers unmistakably. Honeypots, devices for assault examination and zero-day abuse revelation, have been uninvolved in sitting tight for an aggressor. The present study tries to suggest a methodology that involves procedure that has three stages to make it into a successful usage of honeypots taking into account participation amongst honeypots. The system through the methodology programmed distinguishing proof of malevolent exercises would be executed in system. The methodology in this study utilizes strategies for i. Hub verification, ii. Self Healing, iii. Mistake Correction. The suggested programmed systems have been effective as well as require neither past preparation nor information of assault marks so as to distinguish malevolent exercises. Server, Database that is real and data based on Honeypot have been utilized to screen besides to explore the vindictive movement in the system. Server has been utilized for social affair hub data since group leader as well as saves the data in a genuine and information has been depending on the Honey in light of hubs data. Through the helping of this methodology section of new noxious hub would be confined. At long last, three stage procedure presented in this study distinguish pernicious action and gives secure system.

Keywords: Honeypot, Malicious Detection, Security, Monitoring, Log Analysis.

1. Introduction
Because of the expanding intensity of noxious action observed in present days web services, associations have begun to send instruments so as to recognize and react to innovative assaults or doubtful action, known as Intrusion Prevention Systems (IPS). In view of the fact that present IPSes employ principle based Intrusion Detection Systems (IDS), for example,
Snort [1] recognized assaults, they have been restricted to securing, generally, against definitely called as assaults. Accordingly, novel identification instruments have been produced to employ in all the additional intense responsive protection frameworks. The two essential such instruments are considered to be honeypots [2], [3], [4], [5], [6], [7] as well as irregularity discovery frameworks (ADS) [8], [9], [10], [11]. Conversely with honeypots, ADSes and IDSes, present the likelihood of identifying (as well as in this manner reacting to) already obscure assaults, likewise alluded to as assaults related to zero-day. Essentially Safety has not been a state, excluding rather a procedure that implies so as one has to continually enhance and improve safety components to ensure our registering foundation. The researchers in this study have made an attempt to distinguish and break down novel dangers and they have to establish a suitable give quantify counteract aspects. In addition, regardless of the possibility that we make safe our framework alongside as of now recognized dangers, pernicious movement and alleviate vulnerabilities that have been recognized, despite everything researchers require to stress over zero-day (beforehand obscure) assaults. In a later research work [11], there has been a focused thought on this aspect, similarly during the unchangeable time as basically any gadgets with a remote association could be traded off by malevolent clients, and the level of efforts to establish safety for those gadgets has been extremely restricted.

It has been likewise investigated in [12] where roughly US$6 billion had been lost because of digital assaults on the power framework. Subsequently, strengthening barrier instruments to secure these frameworks should be a top priority. To give safety in IT systems it requirement intense technique or framework. Be that as it may, it requires giving safety taking into account the current strings as well as considering the latest dangers. For this sort of safety, specialists have been taking a gander at honeypots as system of misdirection to include an additional layer of safeguard [13]. Honeypots [14] have been considered as ensnares to draw assailants within; these are the material or virtual PC frameworks which impersonate genuine gadgets as well as give substantial checking and action logging, that assists squandering aggressors’ chance and assets and permits protector to think about the assaults and plan the steps that are essential at this stage. Their motivation has been to draw in vindictive clients, think about their exercises and, in the meantime, decrease the assault facade. It is imperative to message so as to in view of the fact that honeypots don't include some other reason, through meaning, some collaboration with those aspects has been viewed as an assault. Subsequently, they don’t display fake optimismism, i.e., all approaching activity has been viewed as malevolent. In a latest study [7], there had been accounted for that an examination honeypot intended to assemble information about assaults on mechanical control frameworks did encounter 4000 assaults in a matter of four days. This study has made a novel attempt to suggest a three stage component in system for recognizing vindictive action and checking noxious movement hub as well as hosts. The commitment put out in this study has been the proposition of a programmed strategy to distinguish system assaults taking into account data traffic gathered via a honeypot.

The following three stage techniques which are i) Node Authentication ii) Self Healing and iii) Error redress. These strategies have been utilized to effectively recognize the primary assaults that has been included in reproduction information set, to proficiently recognize extraordinary malignant exercises from commotion, for example, show parcels and backscatter, that have been a case of real activity which might send fake optimismism. To begin with, a strategy has been utilized for hub confirmation; Second technique has been utilized for recognizing and observing malevolent movement; Finally third has been utilized for expelling malignant hub structure arrange and forestalling new vindictive hub goes into system. In addition, the proposition performs likewise contribution via a replica of the system
movement as signs and clamor information, translating exceptionally connected parts as noteworthy system exercises (for this situation, vindictive exercises).

2. Related Work
In the section of this kind the researchers review the studies which has been related to the territories of honeypots as well as shared strategies on systems. In the data framework asset of honeypot, worthiness mainly depends on unapproved or unlawful utilization [16], albeit different descriptions subsist for particular aspects and functions. Honeypot frameworks have been intended to draw in the consideration of noxious clients with a specific end goal to be effectively focused on and examined by possible assailants, uniquely in contrast to interruption discovery frameworks (IDS) or firewalls that ensures the system against foes. For almost a division system honeypot frameworks consists of certain susceptibilities and administrations that have been usually focused via mechanized assault techniques and pernicious clients, catching information and logs with respect to the assaults coordinated at them. Information gathered at honeypot frameworks, for example, activity catches and working framework logs, has been examined with a specific end goal to pick up data about assault methods, universal risk inclinations and adventures. It is expected that movement and exercises coordinated at frameworks of similar kinds are neither are noxious, as they posses no generation esteem nor run any genuine administration got to by consistent clients.

Due to this trademark (intrinsic to honeypot frameworks) the measure of information caught has been fundamentally decreased in contrast with system IDSs that catch and break down however much system activity as could reasonably be expected. In [15] the researchers have exhibited an opensource HosTaGe low-cooperation portable honeypot. The thought has been to present frivolous convenient honeypots pertaining to mobile gadgets which go for distinguishing malignant gadgets in remote systems. Prisoner bolsters the distinguishing proof of assaults in every single significant convention, e.g., SIP, FTP, Telnet, SMB, MySQL, HTTP and SSH. Through this study the researchers try to upgrade the proposed framework that is twin folded: to start with, aid related to ICS conventions has been included and, second, identifying assaults activated via the similar element has been concentrated and showed in numerous conventions. Likewise, assaults by means of mechanism related to state as well as production relating marks relating to them could be utilized by IDSs have been made official. Amusement hypothesis has for some time been connected to revise system safety, by means of [17], [18] giving broad overviews of the writing. As to utilization of Bayesian amusement molds, Alpcan et al. [19] depicted a safety amusement amongst aggressor and interruption recognition framework in right of entry managed functions. Patcha et al. [20] suggested a flagging amusement for identifying malignant hubs in portable specially appointed systems. Investigation of possible dangers and steps taken in due course in vehicular impromptu systems had been additionally concentrated on in Du et al. [22], wherever a total data diversion model had been explored. In the late years one could see the recommendations in the territory of mark era through the use of honeypots [23], [24], [25]. Case in point, HoneyComb [26] has been deemed a framework which creates a utilization pertaining to the honeyd honeypot to create ready marks. The system is vested with the upside of just utilizing honeypot system activity and in this way decreasing fake optimistics. Nonetheless, as an aftereffect of using honeyd, just abnormal state TCP or UDP data could be analyzed, creating it unacceptable for payload-level examination. Also, either HoneyComb, or any honeypot, can recognize multi-stage assaults.
3. Proposed work
In this study the researchers try to utilize three stage procedures with Honeypot database pertaining to this system. Honeypots symbolize to have congregation-oriented way to deal with the discovery of vindictive movement. They have been utilized to draw in or mistake assailants scanning for recognized aims or susceptibilities furthermore to catch beforehand obscure assaults. So as to check and distinguish malevolent action and hubs in the system, server has been utilized with twin information foundation. One aspect has been the genuine information foundation means where it saves every one of the hubs location and movement of high-quality hubs. Honeypot information base indicates that it saves hubs location and deed of vindictive hub. Process Nodes confirmation, self mending and mistake redress are being recognized as the pernicious movement of system by the assistance of the given databases. In the present day systems have been expanded in all the territory where various brilliant however possibly helpless articles have been sent and website-associated. For instance, shrewd family unit gadgets, meters based on electricity, therapeutic usable gadgets or distant sensors have been in the middle of the main hopefuls. It also additionally runs certain basic functions, for example, information accumulation and continuous observing, that creates them alluring focuses to vindictive aggressors. To give security next to possible assaults, three stage systems have been suggested in the given study. This instrument has not been just utilized for distinguish noxious action hubs additionally another vindictive hubs.

A. Malicious Attack Scenario In Network
There have been assailants who expect to trade off the defenseless focuses to attain their individual addition. A keen aggressor might realize that a straightforward or nonstop assault has been unrealistic to be viable. Henceforth, he/she might attempt to swindle the framework by stirring up his/her activities. This is, a portion of the duration where he/she could do something furtively through putting on a show to be an innocuous client who does typical exercises and sits tight for the following open door. For this situation, one could describe him/her an "inactive" aggressor. At a number of different periods, an additional assailant might dispatch an assault, where one could name him/her a "dynamic" aggressor. In this study the researcher concentrates on the situation for grasp the vindictive aggressor hub furthermore where the guard confronts an obscure assailant with obscure goals.

B. Nodes Authentication
The Fig 1 shows the three step mechanism for malicious node authentication where Hub confirmation is a procedure of gathering hubs connected data and movement and saves it as record records. Amongst different records that might give fascinating data around an aggressor's activity, near to the ground collaboration honeypots generally gather data in regards to the system associations began and coordinated towards them, yielding system stream logs. In the given study gathering and keeping up data about hubs in a system bunching as well as Honeypot server have been utilized. When system is shaped, primary aspect is bunching procedure that is being connected on hubs then hubs have been grouped based hubs data. In the wake of collection hubs taking into account bunch, group lead would be chosen through elite of hubs in that gathering. When bunching has been completed effectively, then group head gathers all hubs data and send solicitation to all hubs in the gathering and sitting tight for reaction of those hubs. All hubs in the gathering have been sending reaction to bunch head for solicitation communication. On the off chance where any hub in the bunch gathering has not been offering reaction to demand of group head after that bunch head would think about as a noxious hub.
At that point bunch head would send all data of solicitation reaction procedure to Honeypot server. Honeypot server gets all hubs data from bunch lead as well as divided data taking into account hubs movement. In the event that hubs data has some noxious movement subsequently with the intention of specific hub data would be put away in database related to Honeypot. On the off chance that hubs data has not been noxious in action subsequently that hubs data is put away in Real information base.

C. Self Healing

Different honeypot techniques have been produced with the objective that the final goal is to discriminate the vindictive action of hubs in system. The given study tries to build up a strategy for self mending to recognize noxious movement and observing action of vindictive hubs. In past stride of hub verification gather as well as transfers hubs data to honeypot server. Taking into account the hubs data it saves hubs subtle element in honeypot as well as database that is genuine. In this case honeypot database keeps up hubs data of which hub hasn’t given suitable reaction of solicitation strategies. When honeypot database acquire the hubs data afterward it would begin to look at conduct of that hubs. In observing occasion it confirms the transferring parcels (information) of hubs whether with the intention of bundle has pernicious data or not. In the event that parcel has malignant data afterward that would be set apart as noxious hub in system else it moves hubs data to database that is genuine as
well as set apart as not childish hubs. Taking into account the given method honeypot database would distinguish malignant hub in the system.

D. Error Correctness

Blunder rightness is third procedure pertaining to this instrument. In the given procedure stamped malevolent hubs have been expelled from system furthermore parcel data of vindictive hubs has been utilized to keep away from new pernicious hub incoming. At the point while some novel hub goes into system after that it would contrast the novel hub data and old noxious hubs information. The above three component are all the more effective to distinguish pernicious hubs and expel that commencing via the systems. This procedure likewise avoids novel malevolent hub section in system.

IV. RESULT AND DISCUSSION

In area of this kind the researchers try to indicate different investigations results concerning the technique for honeypot procedure. In the present days honeypot has been utilized to discover novel assaults, novel infection, and young insects. Similarly honeypot database has been utilized in the framework to find vindictive movement of the hub. In the study, three stage procedures for accomplishing malevolent action of hubs have been suggested. Restring a malevolent action of hubs in system gives a decent security to systems.

![Fig. 2. Comparison process of Proposed and Existing](image)

On the top, the figure 2 demonstrates examination suggested and obtainable procedure. In the suggested mechanism it distinguishes pernicious movement in systems furthermore recognizes novel noxious action superior to anything obtainable mechanism. The suggested study recognizes conduct of vindictive with least time than accessible.
Figure 3 explains accuracy level of proposed system with Honeypot database. Accuracy level of proposed work is better than existing. If nodes count in the network are increasing the average level of accuracy also maintained. In existing work accuracy level is decreasing when no of nodes increasing.

Figure 4 shows network creation. In this process nodes are plotted into network and get id for each node.

Figure 5 shows cluster nodes.
Figure 5 shows grouping of nodes by clustering process. Here nodes are grouped based on energy of nodes and communication links with other nodes.

![Figure 5: Node Grouping](image1)

Fig. 6. Sends Acknowledgement

Figure 6 shows acknowledgement process in the cluster group. Cluster head sends acknowledgement packet to all nodes in the group for identifies the activity of malicious activity. If any node did not reply for acknowledgment then cluster head assume that node is a malicious.

![Figure 6: Acknowledgement](image2)

Fig. 7. Sends malicious information to Honeypot server

Figure 7 explains cluster head forward malicious node and normal node information to Honeypot and real database.

![Figure 7: Malicious Information](image3)
Figure 8 shows monitoring process of malicious nodes activity by Honeypot server. By this process Honeypot finalize the malicious node and store malicious node activity into real database for preventing new malicious nodes entry into the network.

5. Conclusion
Honeypots have been exceptionally fascinating perception situations with the intention of empowering the study to effectively gather noxious information. Be that as it may, not very many endeavors have been as of now completed to exploit these rich data sources. A great part of the exertion has been given to honeypots plan. In this study, procedure of bunching has been utilized to acquire more profundity data of every hub in the system. This procedure has been exceptionally helpful to strategy for Honeypot to recognize vindictive movement. Three stage system of this suggested work executes fine in territory of malignant movement distinguishing proof. Honeypot database has been a capable component to recognize any interruption as well as worms present in the system. Here it has been utilized to find malevolent action as a part of the systems. Look at than obtainable effort the suggested effort executes improved numerous kinds of hubs.

REFERENCES

[1] M. Roesch, “Snort: Lightweight intrusion detection for networks,” In Proceedings of USENIX LISA, (software available from http://www.snort.org/) November 1999.
[2] N. Provos, “A Virtual Honeypot Framework,” In Proceedings of the 13th USENIX Security Symposium, pp. 1–14, August 2004.
[3] D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J. Levine, and H. Owen, “HoneyStat: Local Worm Detection Using Honepots,” In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 39–58, October 2004.
[4] V. Yegneswaran, P. Barford, and D. Plonka, “On the Design and Use of Internet Sinks for Network Abuse Monitoring,” In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 146–165, October 2004.
[5] L. Spitzner, "Honeypots: Tracking Hackers," Addison- Wesley, 2003.
[6] J. G. Levine, J. B. Grizzard, and H. L. Owen, “Using Honeynets to Protect Large Enterprise Networks,” IEEE Security & Privacy, vol. 2, no. 6, pp. 73–75, Nov./Dec. 2004.

[7] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, “The Internet Motion Sensor: A Distributed Blackhole Monitoring System,” In Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS), pp. 167–179, February 2005.

[8] K. Wang and S. J. Stolfo, “Anomalous Payload-based Network Intrusion Detection,” In Proceedings of the 7th International Symposium on Recent Advanced in Intrusion Detection (RAID), pp. 201–222, September 2004.

[9] T. Toth and C. Kruegel, “Accurate Buffer Overflow Detection via Abstract Payload Execution,” In Proceedings of the 5th Symposium on Recent Advances in Intrusion Detection (RAID), October 2002.

[10] M. Bhattacharyya, M. G. Schultz, E. Eskin, S. Hershkop, and S. J. Stolfo, “MET: An Experimental System for Malicious Email Tracking,” In Proceedings of the New Security Paradigms Workshop (NSPW), pp. 1–12, September 2002.

[11] S. Hausman, (2014) “Navigating security threats posed by Internet of Things technology,” [Online]. Available: http://www.securityinfowatch.com/article/11714106/navigating-security-threats-posed-by-internet-oftthings-technology.

[12] S. M. Amin and A. M. Giacomoni, “Smart grid- safe, secure, selfhealing: Challenges and opportunities in power system security, resiliency, and privacy,” IEEE Power Energy Mag., vol. 10, no. 1, pp. 33–40, Jan./Feb. 2012.

[13] W. Zhang and B. Qu, “Security architecture of the Internet of Things oriented to perceptual layer,” Int. J. Comput. Consum. Control, vol. 2, no. 2, pp. 37–45, 2013.

[14] The Honeynet Project, Know Your Enemy: Learning about Security Threats, 2nd ed. Addison-Wesley Professional, 2004.

[15] EmmanouilVasilomanolakis, Shankar Karuppayah, Mathias Fischer, Max M’uhlh’ auser, Mihai Plasoianu, Lars Pandikow, and Wulf Pfeiffer, “This Network is Infected :HosTaGe - a Low-Interaction Honeypot for Mobile Devices,” In Security and privacy in smartphones & mobile devices, pp. 43–48. ACM, 2013.

[16] L. Spitzner, “Honeypots: Catching the insider threat,” In Proceedings of the 19th Annual Computer Security Applications Conference, ser. ACSAC ‘03. Washington, DC, USA: IEEE Computer Society, pp. 170–179, 2003.

[17] T. Alpcan and T. Bas, ar, “Network Security: A Decision and Game Theoretic Approach,” New York: Cambridge University Press, 2011.

[18] X. Liang and Y. Xiao, “Game theory for network security,” IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 472–486, 2013.

[19] T. Alpcan and T. Bas, ar, “A game theoretic analysis of intrusion detection in access control systems,” In Proc. IEEE Conference on Decision and Control, Dec. 2004, pp. 1568–1573.

[20] A. Patcha and J.-M. Park, “A game theoretic formulation for intrusion detection in mobile ad hoc networks,” Int’l J. Netw. Security, vol. 2, no. 2, pp. 131–137, Mar. 2006.

[21] S. Shen, Y. Li, H. Xu, and Q. Cao, “Signaling game based strategy of intrusion detection in wireless sensor networks,” Comput. Math. Appl., vol. 62, no. 6, pp. 2404–2416, Sep. 2011.

[22] S. Du, X. Li, J. Du, and H. Zhu, “An attack-and-defence game for security assessment in vehicular ad hoc networks,” Peer PeerNetw. Appl., vol. 7, no. 3, pp. 215–228, 2012.
[23] Christian Kreibich and Jon Crowcroft, “Honeycomb – Creating Intrusion Detection Signatures Using Honeypots,” In ACM SIGCOMM Computer Communication Review, vol. 34, pp. 51 – 56, 2004.

[24] Urjita Thakar, Sudarshan Varma, and AK Ramani, “Honeyanalyzer – analysis and extraction of intrusion detection patterns & signatures using honeypot,” In Proceedings of the Second International Conference on Innovations in Information Technology, 2005.

[25] Hyang-Ah Kim and Brad Karp, “Autograph: Toward automated, distributed worm signature detection,” In USENIX security symposium, volume 286. San Diego, CA, 2004.