ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Comparative Study of Various Techniques of Attack Handling in Wireless Sensor Network

Dr.Sandeep Singh Kang[1], Amandeep kaur[2]
Professor & HOD[1], Research Scholar[2]
Department of Computer Science
Global Institute of Management and Emerging Technology, Amritsar, Punjab, India

Abstract:
Intrusion is a common issue present within networks. Nodes are connected either strongly or loosely with each other. Users of the network can be malicious in nature. To tackle the issues of intrusion, certain techniques are needed. With the advancement in technology, techniques come into existence to tackle Intrusion within the network. Graph based approach is most common in this regard. This literature provides comparative analysis of techniques used to tackle intrusion within the present system. The comparative analysis helps in selecting best possible technique for detecting intrusion.

Keywords: Intrusion, Network, Malicious, Nodes, Graph

I.INTRODUCTION

Attacks are common and must be handled within the network. Localization is commonly used for this purpose. Localization indicates the management of nodes with fixed or varying distance. The fixed distance between nodes indicates range based techniques and distance higher than particular distance or if distance is not considered than it is known as range free techniques. Sybil attack is one of the common identity based attack. The nodes of different Ids take up the Id of destination and hence node does not get to know to which destination packets is to be transferred. This type of attack degrades the performance of the system and of lifetime of network deceases. The techniques are devised which are used to tackle. Wireless sensor network(WSN) security is prime requirement these days due to its higher need in military as well as civil domains which makes its critical concern. In a *Sybil* attack, wireless sensor network is destabilizing by a malevolent node which uses fake identities in order to interrupt the network's protocols. In attempting to protect WSNs from these attacks, generally graph based techniques are used. According to this graph based technique when we send the data from source to destination if there should be any deadlock occur then it gives the surety but if deadlock will not occurs it means are data will reach safely to destination.

II.LITRATURE SURVEY

[1]WSN is vulnerable to various security attacks when data is sent from source to destination. Source like memory and energy makes it more critical in nature. One of the attacks is Sybil attack in which multiple identities are used to attack the node during transformation of data. In this paper by developing a lightweight system using energy as a parameter for hierarchical WSN. The performance evaluation of this system shows efficiency and scalability for the detection of Sybil attacks.

[2]Sensor nodes gather data from perilous environment and these environments are usually unsecured. In this paper distributed method has been presented by the use of mobile agents and local information of each sensor has to be detected. The result of simulation is used to compare with various their methods.

[3] Wireless sensor network technology is used by both mass public and military to get rid of attacks. The sensor technology is combined with the processing power and wireless communication which makes it more useful in future. The wireless communication technology has to suffer from various types of security threats. This paper comprises of security related issues and challenges in wireless sensor networks. The review of proposed security mechanisms for wireless sensor networks is used to solve this security threats.

[4]Internet of things is used to connect anything at anytime and anywhere which puts an impact on our daily life. Many applications like military region, where sensor nodes are used so that security threats can't occur in the network like black hole, worm hole, hello flood and Sybil attack. One of the most dangerous threats is Sybil attack. In this paper the probability of Sybil free sensor network is calculated subject to the number of sensor nodes and sensor area intensity.

[5] The WSN applications and their access to confidential information, sensed directly or gained from their environments, help them in gaining access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. It is very crucial to provide effective security for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without addressing the security and privacy challenges to ensure that benefits will be achieved easily.

[6]Mobile Adhoc systems (MANET) are a noteworthy cutting edge remote innovation. Progressively and subjectively found hubs convey to each other to frame a Mobile Adhoc Network. MANET is more helpless against various sorts of assault than wired arrange. Dark gap assault is more serious danger to MANET than some other assault. Counteractive action of Black gap assault is finished by finding the vindictive hub before any damage should be possible. Diverse systems are

proposed to anticipate this kind of assault. In this paper these systems are considered with their preferences and hindrances.

[7]A WSN is a framework less sort arrange, which comprises of number of portable hubs with remote system interfaces keeping in mind the end goal to make correspondence among hubs, the hubs progressively set up ways among one another. The nature and structure of such systems makes it alluring to different sorts of assailants. In this paper we examine different sorts of assaults on different layers under convention stack. Distinctive sorts of aggressor endeavours diverse ways to deal with lessening the system execution, throughput. In this paper the vital concentrate is on steering and security issues related with versatile impromptu systems which are required so as to give secure communication. On the premise of the way of assault cooperation, the assaults against MANET might be arranged into dynamic and latent attacks. Attackers against a system can be characterized into two gatherings: insider and untouchable. Though an outcast assailant is not a true blue client of the system, an insider aggressor is an approved hub and a piece of the directing component on WSN.

[8]A Mobile Ad-Hoc Network (MANET) is a framework less or a self-designed gathering of portable hubs that can randomly changes their geographic areas to such an extent that these systems have dynamic topologies and irregular versatility with obliged assets. It more often than not works by communicating the data. Its tendency is communicating so there is an opportunity to disrupt arrange by aggressor. The quantity of assault should be possible in Mobile Ad Hoc Network. This paper examined diverse procedure to recognize and prevent wormhole assault and look at them.

[9] The majority of communicate encryption plans don't give source confirmation property. This enables an enemy to dispatch mimicking assaults. In this way, communicate encryption plot without source verification is not relevant in our genuine as it seems to be. In this paper, we propose a source-confirmed communicate encryption conspire by settling the character based communicate encryption plot proposed by Deliberately. The security of our plan is demonstrated in the arbitrary prophet display. Examination of our plan demonstrates that it is similarly effective as far as calculation and correspondence.

[10] Distributed computing changes the way data innovation (IT) is devoured and overseen, promising enhanced cost efficiencies, quickened development, speedier time-to-market, and the capacity to scale applications on request (Leighton, 2009). As per Gartner, while the buildup developed exponentially amid 2008 and proceeded since, plainly there is a noteworthy move towards the distributed computing model and that the advantages might be considerable (Gartner Hype-Cycle, 2012). Be that as it may, as the state of the distributed computing is rising and growing quickly both theoretically and actually, the lawful/authoritative, monetary, benefit quality, interoperability, security and protection issues still stance noteworthy difficulties. In this section, we depict different administration and sending models of distributed computing and recognize significant difficulties. Specifically, we talk about three basic difficulties: administrative, security and protection issues in distributed computing.

[11] Advances in micro-electro-mechanical systems have triggered an enormous interest in wireless sensor networks (WSN). WSN are formed by large numbers of densely deployed nodes enabled with sensing and actuating capabilities. These nodes have very limited processing and memory capabilities, limited energy resources and it is envisioned that they will be mass produced, to reduce costs. DEEC is a Distributed Energy-Efficient Clustering calculation utilized as a part of heterogeneous remote sensor systems, which utilizes grouping. The bunch heads are chosen by a likelihood in light of the proportion between lingering vitality of every hub and the normal vitality of the system. The hubs with high beginning and remaining vitality will have a greater number of opportunities to be the group heads than the hubs with low vitality.[12][28] It essentially improves the security time of the system by utilizing heterogeneous mindful grouping calculation. This influences the propelled hubs particularly when their lingering vitality diminishes and their vitality comes in the scope of ordinary hubs. For this situation the propel hub passes on rapidly than alternate hubs in the system.

DEEC protocol all nodes use the initial and residual energy level to define the cluster heads. DEEC estimate the ideal value of network[13] lifetime to compute the reference energy that each node should expend during each round. [14]In a two-level heterogeneous network, where we have two categories of nodes, m.N advanced nodes with initial energy equal to Eo.(1+a) and (1 − m).N normal nodes, where the initial energy is equal to Eo. Where a and m are two variable which control the nodes percentage types (advanced or normal) and the total initial energy in the network Etotal.

- The value of Total Energy is given as

$$Etotal = N.(1-m).Eo+N.m.Eo.(1+a)$$

Equation 1: Total Energy Consumed Equation

- The average energy of rth round is set as follows

$$E(r) = \frac{1}{n} E_{Total}\,(1-r)$$

Equation 2: Showing average energy consumed

R denotes the total rounds of the network lifetime and is defined as

$$R = \frac{Etotal}{ERound}$$

Equation 3: Total Rounds

As time advances and innovation propels there is an expanding development of remote interchanges and furthermore of information rates, and with the ceaselessly expanding base of clients of versatile remote correspondences, appeal for broadband has risen and the new utilizations of remote sight and sound are framed the principle motivation to the improvement of the LTE propelled systems. Customary remote frameworks will neglect to take care of the interminably developing demand for range and accessibility. The advancement of D2D innovation is accordingly raised to empower productive and stable correspondence between gadgets through direct movement trade. Coordinate connections between gadgets has many favorable circumstances underneath are a few:

•Data rates: paying little respect to the separation between the gadgets and the cell framework foundation, which can't bolster trading high information rates over long separations, in D2D specialized gadgets can trade high information movement.

•Reliability: D2D correspondence can be utilized to convey straightforwardly regardless of the possibility that the LTE framework falls flat for any reason. •Instant correspondence: in

a D2D correspondence a set number of gadgets can be utilized for moment interchanges similarly walkie-talkies are utilized.

•Less power utilization: utilizing D2D correspondences can diminish the power utilization in light of the fact that if the gadgets are near each other then less power transmission is required.

Comparison of various techniques used to handle attacks

Table.1.Comparison of various attack and handling strategies

Attack/criteria	Details methods	Defensive mechanism
Collision	Misbehavior detection techniques,	• All countermeasures of jamming attack; • Error correction codes(such as CRC codes); • Time diversity;
Resource Exhaustion	Misbehavior detection techniques;	• Limiting the MAC admission control rate[1]; • Random back-offs, • Using time-division multiplexing, • Limiting the extraneous responses, • Protection of WSN ID and other information;
Sinkhole	• False routing information detection; • Cooperating neighboring nodes to each other; • Tree structure and verify by tree; • Verify by visual geographical map;	• Geographical routing protocols ; • Learning global map(if nodes are static and known location); • Scalability; • Probabilistic next hop selection; • Leveraging global knowledge; • Verifying and to trust information that advertised of neighbor nodes; • Authentication link layer encryption and global shared key techniques; • Routing access restriction(R); • Wormhole detection(W); • Key management(K); • Secure routing(S);
Eavesdropping	Eavesdropping is a passive behavior, thus it is rarely detectable ; Misbehavior detection techniques;	• Access control; • Reduction in sensed data details; • Distributed processing • Access restriction; • Strong encryption techniques;
Wormholes	• False routing information detection; • Wormhole detection; • Combinational methods; Packet leashes techniques;	• Packet leashes techniques; • MAD protocol and OLSR protocol; • Directional antennas; • Multi dimensional scaling algorithm(scalability) • Using local neighborhood information; • DAWWSEN protocol; • Designing proper routing protocols(clustering –based and geographical routing protocols); • Leverages global knowledge; • Verifying information that announce of neighbor nodes; • Graphical position System; • Ultrasound;

III. RESULTS FROM EXISTING LITERATURE

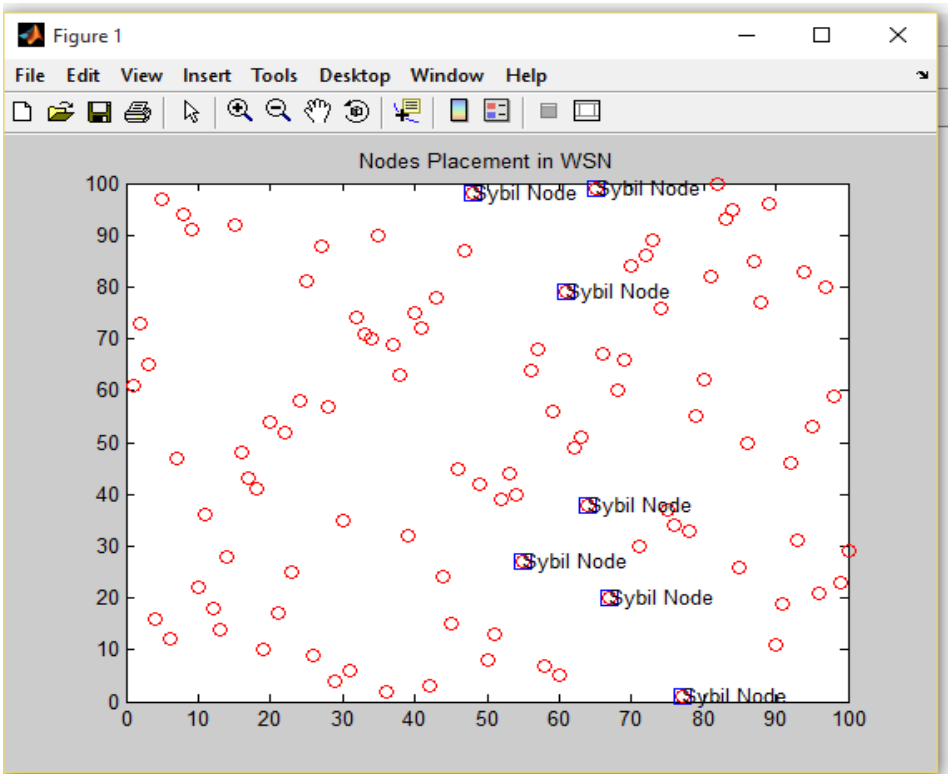

Figure.1. showing sybil nodes

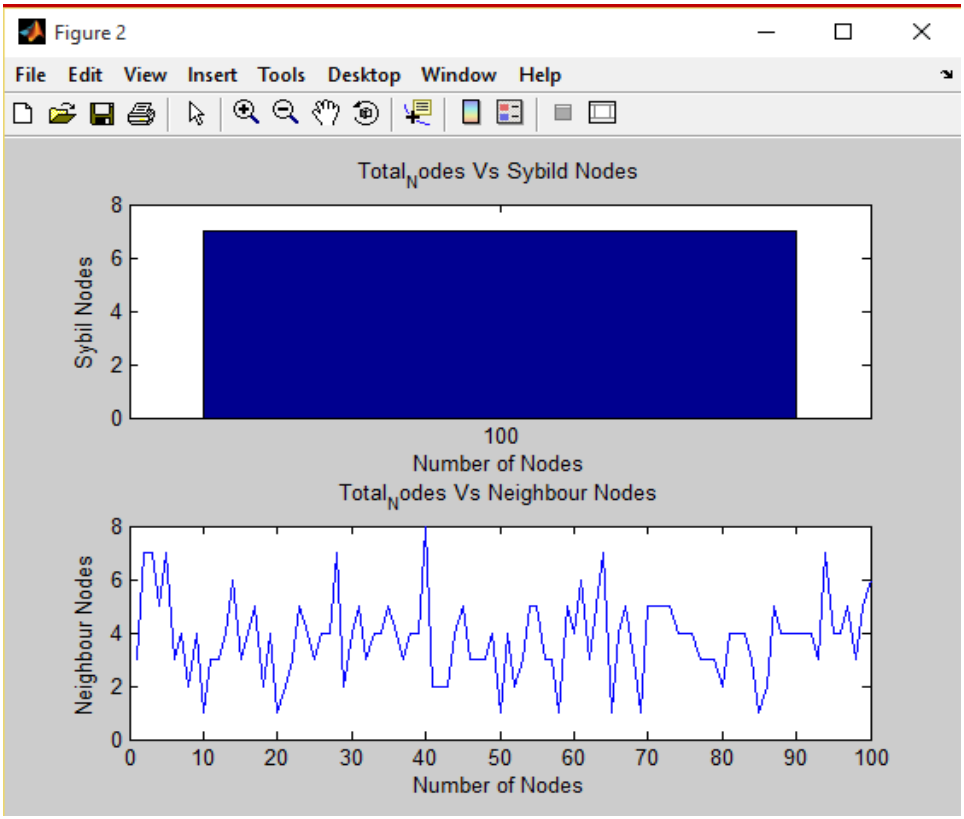

Figure.2. describing out of hundred only seven nodes are detected as sybil
The problem with the existing approach is that only nodes are detected without the location.

IV.CONCLUSION

In this paper we analyse the various techniques used for intrusion detection in WSN. The comparative study of various techniques will result in identifying the better and extensive security mechanism to secure WSN. By using Graph based mechanism in our paper we protect our data from Sybil attack.

V.REFERENCES

[1]. N. Alsaedi, F. Hashim, and A. Sali, "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks," no. Micc, pp. 91–95, 2015.

[2].S. Moradi, “A distributed method based on mobile agent to detect Sybil attacks in wireless sensor networks,” pp. 276–280, 2016.

[3]. a. S. K. Pathan, H.-W. L. H.-W. Lee, and C. S. H. C. S. Hong, “Security in wireless sensor networks: issues and challenges,” 2006 8th Int. Conf. Adv. Commun. Technol., vol. 2, p. 6 pp.-pp.1048, 2006.

[4].P. Sarigiannidis, “Analysing Indirect Sybil Attacks in Randomly Deployed Wireless Sensor Networks,” pp. 0–5, 2016.

[5].S.-H. Yang, “WSN Security,” pp. 187–215, 2014.

[6].D. Mishra and S. Arukonda, “Black Hole Attack Prevention Techniques in MANET : A Review,” vol. 3, no. 6, pp. 6735–6738, 2014.

[7].Gagandeep, Aashima, and P. Kumar, “Analysis of different security attacks in MANETs on protocol stack a-review,” Int. J. Eng. Adv. Technol., vol. 1, no. 5, pp. 269–275, 2012.

[8].Y. Gohil, S. Sakhreliya, and S. Menaria, “A Review On : Detection and Prevention of Wormhole,” vol. 3, no. 2, pp. 1–6, 2013.

[9].M. Luo, C. Zou, and J. Xu, “An efficient identity-based broadcast signcryption scheme,” J. Softw., vol. 7, no. 2, pp. 366–373, 2012.

[10].J. Sen, “Security and Privacy Issues in Cloud Computing,” arXiv Prepr. arXiv1303.4814, no. iv, 2013.

[11].R. Stoleru, T. He, and J. A. Stankovic, “Range-free localization,” Secur. Localization Time Synchronization Wirel. Sens. Ad Hoc Networks, pp. 3–31, 2007.

[12].T. Tiwari and N. R. Roy, “Modified DEEC: A varying power level based clustering technique for WSNs,” 2015 Int. Conf. Comput. Comput. Sci. ICCCS 2015, pp. 170–176, 2015.

[13].V. Devadevan and S. Suresh, “Energy Efficient Routing Protocol in Forest Fire Detection System,” 2016 IEEE 6th Int. Conf. Adv. Comput., pp. 618–622, 2016.

[14]. T. N. Qureshi, N. Javaid, M. Malik, U. Qasim, and Z. A. Khan, “On performance evaluation of variants of DEEC in WSNs,” Proc. - 2012 7th Int. Conf. Broadband, Wirel. Comput. Commun. Appl. BWCCA 2012, pp. 162–169, 2012.