Node Validation Technique to Increase Security of Wireless Sensor Networks

Parveen Singla, Gaurav Mehta, Rinkesh Mittal, Vinay Bhatia

Abstract*: A distributed sort of network in which sensor nodes can join or leave the network when they want is identified as wireless sensor network. Due to self-arranging of the network, attacker nodes make their entry inside networks and launch different types of active and passive intrusions. The active attacks can be divided into various sub categories and one of them is misdirection attack. This attack increases delay in the network. The available attacker hub will trigger attack. In order to recognize and disengage malicious nodes a novel strategy is proposed in this work. The malicious nodes are recognized from the networks which are in charge of triggering the node. The attacker or malevolent node launches sinkhole intrusion. This intrusion streams fake recognition information within the network. This study proposes a verification approach for detecting attacker nodes present in the network. The performance of introduced approach is tested in NS2. It is scrutinized that performance is improved as per various parameters.

***Index Terms*: ACTIVE ATTACKS, DOS,IDS,LEACH,NS2, SINKHOLE, WSN,**

I. INTRODUCTION

A combination of small light weight wireless sensor makes a Wireless Sensor Network. The limited storage of energy and limited capabilities of processing of sensor nodes make it cheaper in price. This network comprises numerous sensor nodes, sometimes hundred or even thousands. This network is extremely distributed and positioned in hazardous situations [1]. This network observes environs through the measurement of physical factors such as moisture, heaviness and temperature. These networks are extremely applicable for certain applications such as natural life scrutiny, army, smart exchanges, contemporary attribute handling, and insight of fundamental bases, radiant configurations, distributed independence, mobility monitoring, analyzing person's heart beat etc. Energy of battery is utilized by sensors in form of energy resource. Battery is a limited power resource. These networks are generally prone to various attacks, therefore the deployment of sensor nodes randomly can be harmful [2]. Therefore, planned consumption in this network is consistently an important issue. Thus, this network should have power efficient plans for increasing life span of these networks.

Revised Manuscript Received on June 15, 2019.

Dr. Parveen Singla, Department of Electronics & Communication Engg. Chandigarh Engineering College, Landran, Punjab, India.

Gaurav Mehta, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India.

Dr. Rinkesh Mittal, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India.

Dr. Vinay Bhatia, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India.

There is need to develop an inherent sharing system for improving network's life span by increasing network throughput and decreasing transmission delay.

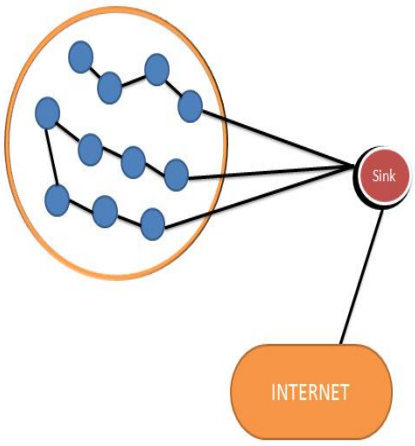

Fig. 1: Wireless Sensor Network

These networks are generally deployed in unfriendly and hazardous topological conditions. In this environment, security is the major concern. These networks can suffer from several physical and rational intrusions in these kinds of circumstances. In these networks, security is extremely significant. In general, these networks generate alerts. These alerts need abrupt consideration [3]. Fake alerts made by these networks can cause unnecessary measures. There are various attacks which have been faced in wireless sensor network. An attacker node records packet at some specific location within the network during wormhole attack. After that they get channel to another location. The disruption is created in this when tunneling and routing take place in control messages. The intrusion generally affects network layer. By monitoring the network and using flexible routing scheme this problem can be prevented. A set of nodes within the network are captured and reprogrammed by attacker node in black hole attack. It will not forward that packet to the base station instead of that it will block the packets. The attacker node captures that packet that makes its entry in black hole area. The attacker node prevents this packet from reaching the destination node. In Denial of Service Attack, the availability of all nodes gets affected by malevolent node. The major objective of this intrusion is to obstruct the sensor nodes' tasks [4]. In this attack, battery absorption technique and radio signal congestion is implemented by malevolent. Byzantine Attack uses an intermediary compromised node for launching intrusions. On non-optimal paths, the collision forwarding of packets occur which causes dropping of packets selectively. This all result in routing services interruption or dreadful condition. In Jamming attack, the radio frequency used by sensor node gets

RetrievalNumber:I11380789S19/19©BEIESP
DOI: 10.35940/ijitee.I1138.0789S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

inferred. At which destination node is getting signal from the sensor is verify by attacker. In the beginning, the frequency at which target node receives signal from source node is monitored by malicious. The signal is transmitted by attacker on this frequency. This signal is very strong and disrupts the functioning of whole network. By monitoring and finding that frequency the attacker transmit signal on that particular frequency which is very powerful that network can be disrupted by it [5]. In Collision Attack, the attacker will find frequency and then sends data on that same frequency which will occur in collision of packets and data need to be retransmitted again. In Man- in- the- middle attack, the attacker will sit in between sender and receiver. So whenever, sender passes any information the attacker will capture this information. In some cases, the malevolent can act as authentic sender. Because of this, even receiver will get masquerade and communicate with the receiver. In Misdirection Attack, the data packet is sent to a different location other than the actual destination. The attacker will misguide the packets. This will result in increase in time of packets to reach at the destination and the system gets degraded [6]. The existence of selfish nodes within the network misguides packets. All of these issues lead to decrease in efficiency. In Node Replication attack, the malevolent node is added in the network by malicious. This is done by assigning the Node ID of some existing node to this malevolent node. A scenario in which the attacker sends or replays the hello packets with the help of high trans-mission power for discovering the neighbor packet is said to have a hello flood attack. This helps in creating an illusion for the other nodes that the attacker is their neighboring node. This might further result in disrupting the routing protocol and causing other attacks also within the same network. The malicious node is selected as a parent node due to its ability to transmit packets with higher power. The messages that are to be broadcasted across the network are then passed through this parent node. This results in causing delay within the network. Inside wireless sensor network, the malevolent sends hello messages to various nodes. The attacker node is thus convinced to be as the neighbor node by these various nodes within the network [6]. The nodes sends reply messages in response of these Hello messages. This results in the depletion of energy. There is also a confusion state caused within the network.

The attack in which one malicious node generates numerous identities is known as a Sinkhole attack. Due to the various characteristics of wireless sensor networks, this attack is highly vulnerable to these networks. They also result in generating a gateway to all the other various attacks. Within the peer to peer networks, the sinkhole attack was introduced which caused the generation of various issues within the network [7]. The issues arising here mainly are related to distributed storage, voting, resource allocation and various such operations going on within these networks. However, the traditional security related techniques could not ensure that all such problems could be avoided as they had the limited sensor nodes present in them. Thus, there is a need to make enhancements within this method yet.

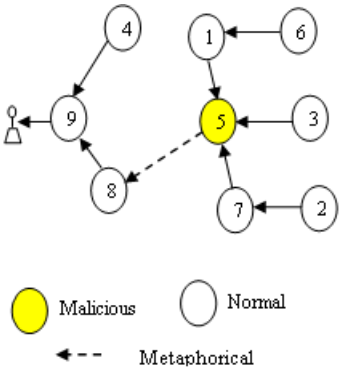

Fig. 2: Sinkhole Attack Scenario

II. LITERATURE REVIEW

Mayank Kumar Sharma et.al proposed a study of resource depletion attack on WSN which is commonly known as Vampire Attack [8]. A mitigation technique is also proposed which identify the vampire nodes and segregates the sensor nodes from the network of sensor. These whole procedures save the energy of the victim nodes. There are two types of vampire attack technique have been diagnosed. The sensing unit senses the units and parameter to diagnose the system regarding their applicability. Lack of accessories, money, man power and energy makes it less secure and inadequate for their functionality. The vampire attack is basically a source depletion attack on WSN. Hence, the study concludes that the proposed approach is completely able to mitigate the effect of two Vampire nodes; an improvised form of victim nodes can also be explained.

Aditi Rani et.al proposed a novel security algorithm which provides confidentiality by protecting the data from being misused. In this technique each node is identified by the integer number between 1 to N [9]. The data can be encrypted and decrypted according to the integer number assigned to each node. It consumes more energy and money which is the big demerit of this scheme. They do not provide any secured network and do not reduce the complexity of the system at this time. Hence, the propose algorithm concludes that it is simple, unique, require less space, time and money and protects from various threats related issues.

AminaMsolli et.al proposed a new key pre-distribution scheme works according to the identification and modification of the initialization phase N [10]. It makes sure about the elasticity of the captured nodes attack. The security Of WSN requires protected messages between sensor nodes. In the respective paper key pre-distribution scheme ensures the security of wireless sensor networks. This scheme is based on the changes occur in the initialized time. It manages the technical security in WSN. The issues regarding security of these wireless sensor networks makes is less versatile and difficult to handle. The networks are made more secured and ensure the shared and stored data and information should be properly secured. Hence, the author concludes that this scheme is more efficient for flexibility in comparison to the any other schemes as the simulations performed.

Janhavi Kulkarni, et.al proposed On-Chip Crystallographic unit for the implementation of the security at very low cost. It reduces the operational time and computational complexity of security in WSN [11]. The proposed method is most suitable approach in order to solve the security related

issues. However, it is not easy to implement, it contains lots of flexibility without compromising the need of information security. Use of this processor should be workable choice for the implementation of the security in WSNs. The system affords the designer freedom to decide the amount of security required for the optimization of the system. Hence, the proposed technique results that without any loss in security units like key space and adversary's advantage, achieves a low cost and low complexity solution.

C. Anand et.al has concluded that WSNs have to face few security attacks that influencing the execution of network. This security issues come due to number of issues such as resource constraints, their deployment in distant region and many more. This attack will misuse the transmission to deny the access of resources given above. In this paper the authors have proposed one mechanism in order to determine the DoS attack issues. This was done by implementing intruder detection approach, key mechanism with the help of retracing of routing paths and node validation scheme. By determining the DoS attack providing the secure and reliable transmission of data is the main reason of proposing that scheme [12].

Omar Said et.al proposed a novel approach. This apprcoach deployed heterogeneous sensors in 3D wireless sensor networks (WSNs). The single sensing and multiple sensing are the two sensing situations which are handled by that proposed model. The most reliable sensor deployment has been done with respect to some critical parameters such as nature of-administration or Quality of services (QoS). The authors have also given WSN proficiency in terms of various probabilistic distributions. A simulation domain for testing the proposed model used is OPNET and NS2. The simulation outcomes indicated that the best results were obtained by using Gaussian distribution as evaluation approach. The results were obtained using uniform technique. It also has been seen that there is minimal execution in case of chi-square and beta WSNs [13].

III. RESEARCH METHODOLOGY

The network performance is reduced by the malicious node. The malicious node causes various types of active and passive attack by entering the network. One of the active types of attack is sinkhole attack in this attacker node floods the network with rough packets and sensor nodes keep on busy to send route reply packets. In this network to isolate malicious nodes to enter a mutual authentication based technique will be proposed in this work.

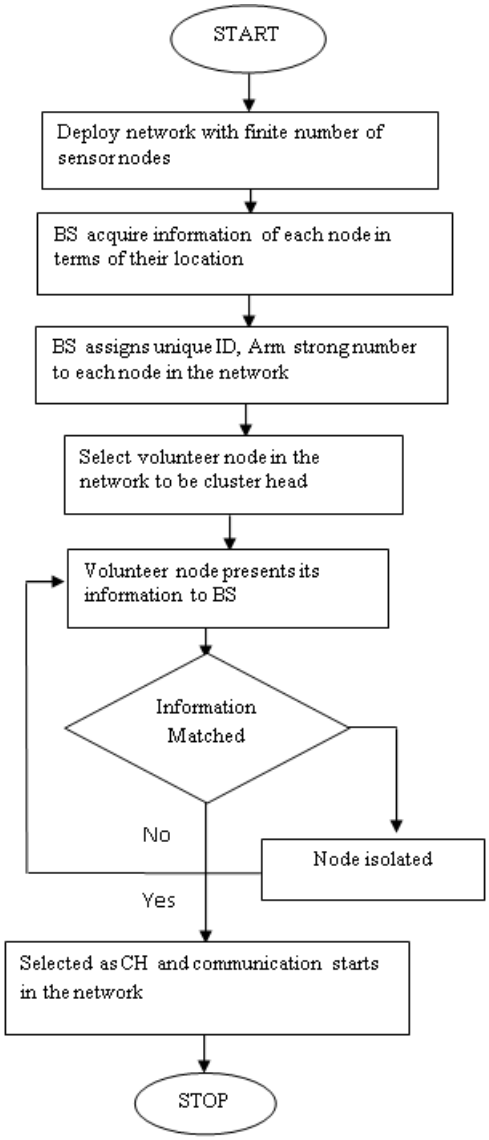

Fig 3: Proposed Flowchart

IV.EXPERIMENTAL RESULTS

The obtained outcomes are applied in NS2. The proposed and existing approaches are compared for the evaluation of results on the basis of some parameters.

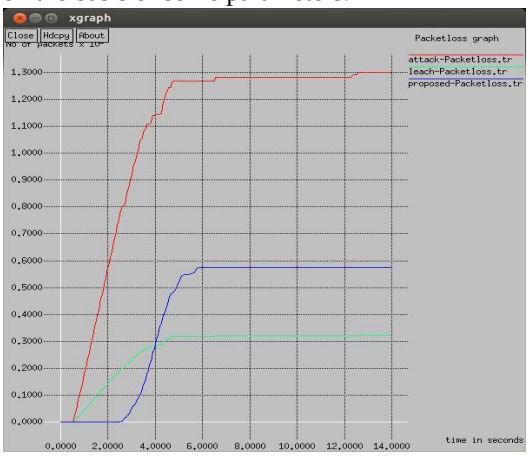

Fig 4: Packet loss comparison

As shown in figure 4, the value of the basic leach, leach protocol under the impact of sinkhole attack and

projected technique is compared in terms of packet loss. It has been analyzed that LEACH protocol is maximum effect and packet loss is reduced in the network after isolation of sinkhole attack.

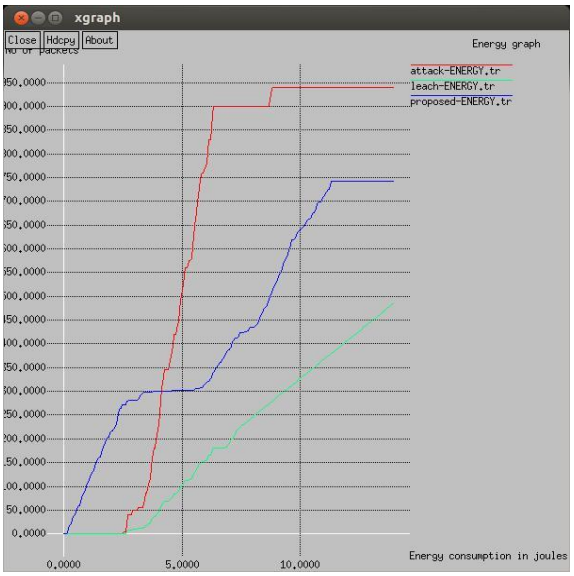

Fig 5: Energy Comparison

As shown in the figure 5, the energy consumption of the proposed technique, LEACH protocol and LEACH protocol under the impact of sinkhole attack is compared and it has been examined that power consumption is decreased after attack isolation.

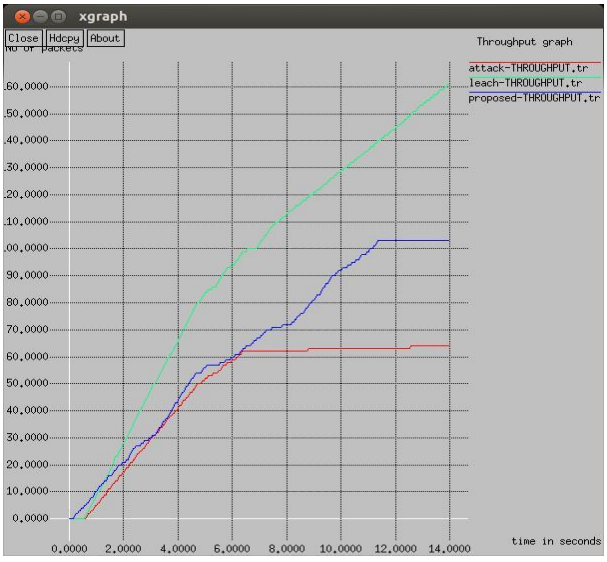

Fig 6: Throughput Comparisons

As shown in the figure 6, the throughput of proposed, LEACH protocol and LEACH protocol under influence of sinkhole attack is depicted and it is examined that network throughput is increased at steady rate after attack isolation.

V.CONCLUSION

In this paper, it is been concluded that LEACH protocol is one of the most effective protocol to decrease power utilization of wireless sensor network. In this thesis work, the mutual authentication approach has been proposed for the detection and isolation of attacker node from the network. The performance of prohected technique has been scrutnized in terms of packet loss which is reduced to 15 %, network energy consumption is reduced to 18 percent and network throughput is increased to 25 percent. In this research work, a novel appraoch is proposed for identifyng and isolating attacker node from the network. In this network, the delay per hop is scrutnized by base station as per the threshold level. The atacker node is recognized using delay. The node causing maximum delay is identified as attacker node. This phenomenon reduces power utilization and delay within the network. This phwenomenon increases network throughput as well.

REFERENCES

[1] Omar Banimelhem, Muhammad Naserllah, and Alaa Abu-Hantash, “An Efficient Coverage in Wireless Sensor Networks Using Fuzzy Logic-Based Control for the Mobile Node Movement,” 2017, IEEE

[2] RanuShukla, Rekha Jain, P. D. Vyavahare, “Combating against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network”, 2017, Recent Innovations is Signal Processing and Embedded Systems (RISE)

[3] Poonam Rolla, ManpreetKaur, “Dynamic Forwarding Window Technique against DoS Attack in WSN,” 2016, IEEE

[4] Aamir Shaikh and Siraj Pathan, “Research on Wireless Sensor Network Technology”, 2012, International Journal of Information and Education Technology, Vol. 2, No. 5

[5] RakshaUpadhyay, Salman Khan, HarendraTripathi, Uma Rathore Bhatt, “Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain,” 2015, IEEE

[6] Yogesh Kumar Fulara, “Some Aspects of Wireless Sensor Networks”, 2015, International Journal on AdHoc Networking Systems (IJANS) Vol. 5, No. 1

[7] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, “A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks” Journal of Security Engineering, 2014, pp.241-250

[8] Mayank Kumar Sharma, Brijendra Kumar Joshi, “Detection & Prevention of Vampire Attack in Wireless Sensor Networks,” 2017, IEEE

[9] Aditi Rani, Sanjeet Kumar, “A Low Complexity Security Algorithm for Wireless Sensor Networks,” 2017, IEEE

[10] AminaMsolli, HaythemAmeur, AbdelhamidHelali, HassenMaaref, “A new secure key management scheme for wireless sensor network,” 2017, IEEE

[11] JanhaviKulkarni, Karan Nair, AdityaPappu, SarthakGadre, Ganesh Gore, Jonathan Joshi, “Using On-Chip Cryptographic Units for Security in Wireless Sensor Networks,” 2017, IEEE

[12] C. Anand, R. K. Gnanamurthy,” Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network”, 2016 Springer Science + Business Media New York

[13] Omar Said and AlaaElnashar,” Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments”, 2015 Springer

AUTHORS PROFILE

Dr. Parveen Singla, did B.Tech in Electronics and Communication Engg. from Hindu college of Engineering, Sonepat affiliated to Maharishi Dayanand University, Rohtak in 2003 and M.Tech in Electronics and Communication Engg from N.C College of engineering, Panipat affiliated to Kurukshetra University, Kurukshetra in 2008. He did PhD in ECE from IKGPTU in 2016. His total teaching & research experience is 15 years. Now he is working as Associate Professor in Electronics & Communication department in Chandigarh engineering college. He has more than 20 publications in various reputed journal/conferences. His research area includes wireless communication and soft computing.

Gaurav Mehta, Research Scholar,Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, Indiamehtag781@gmail.com

Dr.Rinkesh Mittal, Associate Professor, Department of Electronics & Communication Engg., Chandigarh Engineering College, Landran, Punjab, India
hod.coeece@cgc.edu.in

Prof.(Dr.) Vinay Bhatia is a B.Tech, M.Tech, Ph.D in Electronics and Communication Engineering. Currently he is serving as Professor and Head, Department of Electronics and Communication Engineering at CGC landran. He has authored about 90 research papers in various national/international conferences/journals. Currently he is working on routing and security issues pertaining to wireless networks. His main research interests include mobile and adhoc wireless networks, wireless mesh networks and wireless securities