International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

A Research on the Malicious Node Detection in Wireless Sensor Network

Nagarjun S , Santosh Anand , Somnath Sinha

Abstract: ***Wireless Sensor Network (WSN) has been looked into broadly in the course of recent years. WSN were first utilized by the military for reconnaissance purposes and have since ventured into modern and regular citizen uses, for example, climate, contamination, traffic control, and human services. There are a few research difficulties, one part of remote sensor arranges on which inquire about has been directed is the security of remote sensor systems. These systems are powerless against programmers who may assault in WSN. A case of this would be an adversary seizing an automaton and inspiring it to assault inviting powers. In this proposed work, security for WSN is concerned. Detection of a fake node in the network is the main part. Using common scenarios, we can spot an attack and a malicious node in the network. By calculating the packet drop, throughput, and residual energy. These are demonstrated in ns2, thereby proposed scheme helps to achieve in detecting the fake node.***

Index Terms**: *Energy, Packet drop, Throughput, Wireless sensor network.***

I. INTRODUCTION

WSN is primarily utilized in military applications to convey between hubs to a base station (control room), presently multi day's WSN can be utilized in the field of backwoods fire location, contamination control, etc [10]. The sensor hubs are savvy, with the goal that it is progressively well known in the systems administration to impart from hubs to sink. This exploration venture depends on WSN look into difficulties, which is conveyed in the plane region, where a human can't reach and there are no offices to revive the battery of sensor hubs and chances are less to supplant the sensor hub. At the point when there is battery consumption happens the sensor doesn't work with the goal that we propose some vitality productive conventions to accomplish them. Wireless sensor networks (WSN's) are shaped by a lot of hubs that assemble data and forward it to sink. A sensor hub is smaller, application explicit, has low vitality needs and has abilities to detect ecological changes, flag preparing and remote correspondence. The potential preferred standpoint of organized detecting over the traditional methodology can be abridged as more prominent inclusion, exactness and unwavering quality at a conceivably lower cost. Other than the benefits of sending a WSN in basic applications, one ought to know about the impediments and difficulties. One of the prime worries in WSN is information security. The data that the sensor gets, should be prepared and transmitted to the sink, which is then given to the base station and is accessible for the end clients by means of the web. WSN is defenseless against security assaults due to the communicated idea of the transmission medium. How far the information is solid relies upon the dimension and kind of security that has been incorporated to keep it from any outsider interloper gaining admittance to those indispensable data and being abused. Based on the area of the assailant, attacks can be arranged into two kinds [11]:

1. External attacks: External attacks are chiefly done by a node that does not have a place or outside the system. They gain admittance to the system by a few methods and once they gain admittance to the system, they begin sending counterfeit bundles, wrong steering data and cause forswearing of administration in a request to disturb the execution of the entire system.

2. Internal attacks: In inside attacks, the aggressor has ordinary access to the system just as takes an interest in the ordinary exercises of the system. The assaulter enters in the network as a new hub either by trading off a current node in the system or by malicious personalization and begins its malicious conduct. Interior assaults are more hazardous than the external assaults: since the traded off node are initially the favorable clients of the specially appointed system that is an ad-hoc network, they pass the confirmation system effectively and get insurance from the security systems. When an attack is there then the workflow in the network changes, so detection for that malicious node is important, in this proposed method there will be two networks with attack and without attack. By comparing both the results we can detect the malicious node.

II. RELATED WORK

Wendi Rabiner Heinzelman et al, 2000 [1] LEACH (Low Energy Adaptive Clustering Hierarchy) protocol was implemented by the authors in this work. LEACH, clustering based protocol which decreases energy dissipation in a sensor network. LEACH, is self-organizing and uses an adaptive clustering protocol. And distributes the energy charge equal to the WSN sensors. LEACH will also do the random movements which have a high relative - energy cluster head location, so the cluster head rotates between the different WSN sensors in order not to drain the node's battery. Fan Xiangning et al, 2007 [2] describes about multi-hopLEACH and energy LEACH protocol. Energy-LEACH advances in the selection of finding the new cluster head. In the next round which node have the highest energy, then that node will be cluster-head.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Nagarjun S, Department of Computer Science, Amrita School of Arts & Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India.
Santosh Anand, Department of Computer Science, Amrita School of Arts & Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India.
Somnath Sinha, Department of Computer Science, Amrita School of Arts & Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India.

Multihop-LEACH gets improves in the communication like from single hop to multiple-hop in between cluster-head and a sink. In this work, authors concluded that multihop-LEACH and energy LEACH have good performance as compared to LEACH protocol. In energy LEACH protocol first round of communication, all the nodes have the same chance to turn as cluster head. Delan Alsoufi et al, 2012 [3] described about security for WSN. The author proposed a new protocol LEAP(Localized Encryption and Authentication Protocol). LEAP protocol uses µ-TESLA type to provide broadcast in base station authentication. The author generates Four keys they are: individual keys, pair-wise keys, cluster keys, and group keys. In this work, author used fifty WSN sensor nodes placed randomly. Initially, an individual-key was used for all nodes from a randomly generated by a master key. Cluster-key was created by single node and given to their neighbouring nodes. Finally, global-key was created in order to permit public broadcasts. Jianpo Li et al, 2017 [4] proposed DV-HOP algorithm for wormhole attack. First, algorithm creates the neighbour node relationship by using broadcast flooding technology. Suspect beacon node can be seen by relating to the theoretical and neighbour node in the network. Later, doubtful beacon node calculates the distance for other beacon nodes. Using the neighbour node relationship list (NNRL) it finds the actual beacon nodes which is affected. Beacon nodes in the different locations. Wormhole attacks marked one or two. Later, the unfamiliar node mark by themselves as one or two allowing to the beacon node marked before. In the next round, the nodes marked by one and the node marked as two divided from each other. To the work finally, authors got an outcome as advanced DV-hop technique reduced by about 80% compared to DV-hop algorithm against wormhole attack. Amar Rasheed et al, 2012 [5] working on three-tier security scheme. In this work, author uses pairwise keys to its basic components and another two separate keys types. For mobile sink one to get access of the network, the second one for establishing pairwise key in between the sensor nodes. Main concentration done here is to get a better authentication technique between sensor nodes and the stationary access node. As compared to single polynomial approach this work gave better network flexibility against mobile sink attack. In this works authors got better security performance for the proposed technique against sensor nodes and stationary access nodes. S. Misra et al, 2010[6], the creators proposed a decentralized procedure to identify character based assaults. The creators managed the reality that as long as the battery is releasing the transmitted control continues diminishing. A 8-step discovery system was proposed: a hub sends a demand to join a WSN and picks the transmission channel. The new hub's neighbors produce the new hub's flag print by tuning to the past channel. At that point, every hub computes the RSSI esteem and communicates it to whatever remains of the new hub's neighbors. Each hub produces the RSSI vector that speaks to the new hub by joining all the got RSSI values which are estimated intermittently. At last, when a strange RSSI esteem is gotten which demonstrates a conceivable interruption, another RSSI vector is created. A short time later, the two vectors - the former one what's more, the recently produced one - are contrasted with identifying the interruption.

III. SIMULATION

Simulation of malicious node detection is implemented in a Network simulator (version 2.35) is popularly known as NS2. To create a malicious node, we used AODV protocol [12], by creating 50 nodes. Simulation scenario in NS2 is represented in Fig. 1. Network parameters are given in table 1.

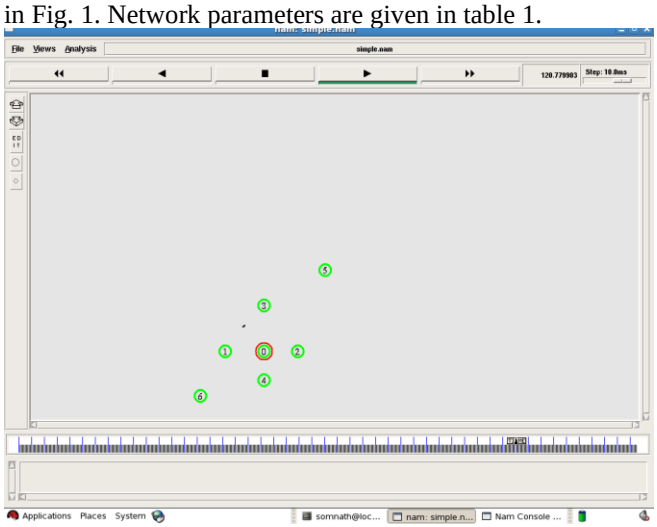

Fig. 1. Simulation scenario with 7 nodes and 2 malicious nodes with a random distribution.

Table 1: Simulation Parameters.

Parameters	Values
NS2	Versions 2.35
Simulation area	500x500 (sq. m)
Simulation time	80,90sec
Mac Layer	802.11
Routing protocol	AODV
No of Nodes	7
Malicious Nodes	1-2

To detect a fake node in a network we have used the following parameters throughput, packet drop and energy consumption of each node. These are the most extensive parameters used in WSN.

Throughput: Rate at which data sent successfully over a given time period from one node to another. It usually calculated in Kbps, Gbps, Mbps, and Bps.

Packet drop: The number of packet loss while communication happening in the network. If any attack is there in a network, then the high chance of packet drop occurs.

Residual energy: Each node will have initial energy, at the time of the packet send or receive the energy of a node will be reduced. And the current energy of a node after send or receive is called residual energy.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

IV. RESULTS AND ANALYSIS

The detection of malicious node takes place in the WSN environment, the organization of these nodes is random in nature. Initially when there is no attacker in the network, the throughput will be good, there is no packet drop, and takes how much energy the node needs to send or receive a packet. If there is an attacker in the node, then all three will vary. i.e. throughput will decrease, packet drop will be high, and the node which is affected its energy will be used more.

Fig. 2. Shows how throughput values decreased compared to its initial stage of deployment. Hence it shows there will be an attack and a malicious node in the network.

Case1: when there is no attack.

In this case, network will have expected (high) throughput because the source can communicate with a sink without any disturbance.

Case 2: when one node is malicious.

In this case, throughput will be affected because the malicious node will try to communicate with the non-malicious node to reach the sink which will decrease the throughput of the network.

Case 3: when two nodes are malicious.

It is like case 2, but there will be two malicious nodes and performance will decrease more than that.

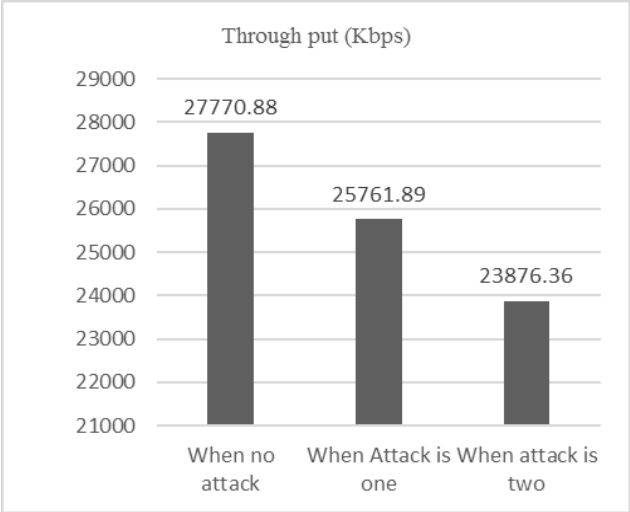

Fig. 2. Throughput values with and without attack.

Fig. 3. Shows how much packet is loosed while communication happens in the network. When there is no attack the packet drop is less, as compared to when there is an attack in the network. This is another parameter which strongly tells there is an attack and a malicious node in the network.

Case 1: when there is no attack

In this case, there will be zero packet loss because there is no attack in the network so that the source node can easily communicate with the sink node.

Case 2: when one node is malicious

In this case, malicious node will drop the packets as it cannot communicate with the sink because of the attack.

Case 3: when two nodes are malicious

This is like case 2, in this case packet drop will be more because two nodes will drop the packets.

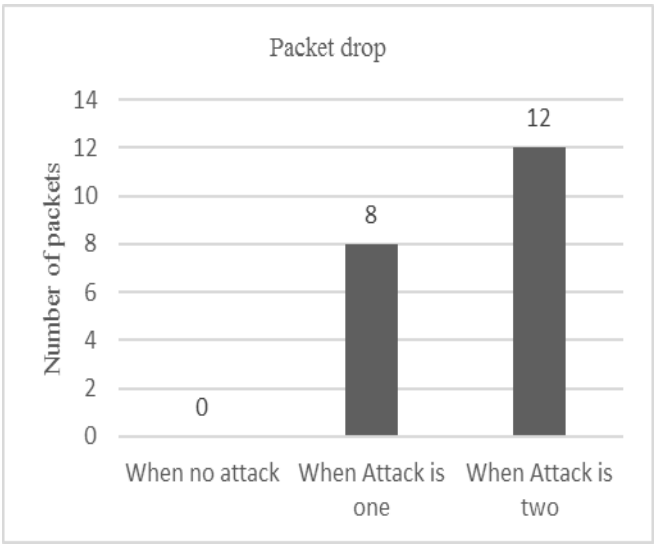

Fig. 3. The number of packets drop with and without attack.

Fig .4. Shows the energy level of each node when there is no attack. It takes minimal energy while communication.

Case 1: when there is no attack

When there is no attack in the network it will consume normal energy, according to transmission and sleep mode. In this case, node will not waste (consume unnecessary) energy.

Case 2: when there is an attack

In this case, malicious node will consume more energy because it will try to communicate in every communication to transmit the packet, which will lead to more energy consumption in the network.

This is another parameter which confirms that an attack and a malicious node in the network.

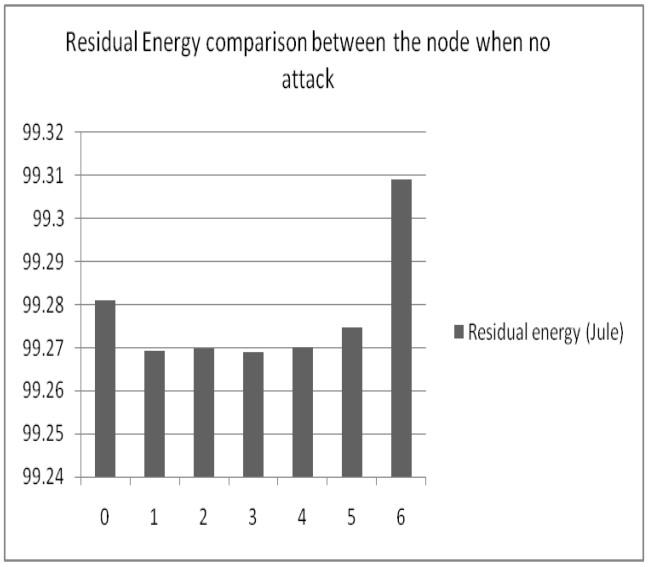

Fig. 4. Residual energy consumption when there is no attack.

Fig. 5. Shows the energy level of each node when there is an attack. If the node is malicious then it takes more energy.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

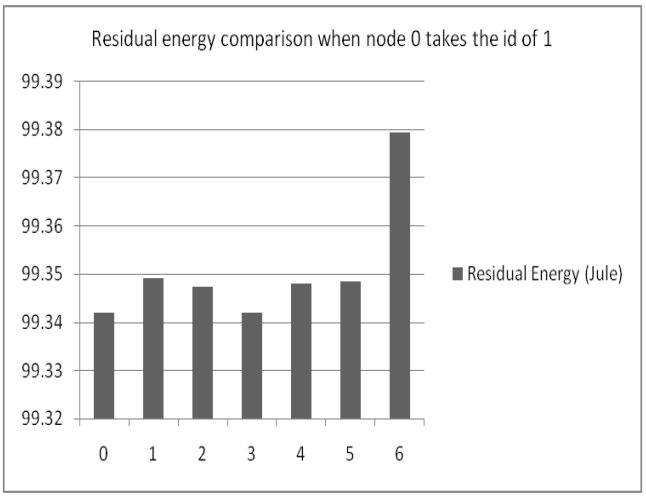

Fig. 5. Residual energy consumption when there is an attack.

V. PROPOSED METHOD

Energy is an important factor in WSN. This is the limitation of the nodes in WSN also. Most of the attacks are generated by targeting this limitation. That's why here this parameter is used as identifying the attack. Here when the comparison is taken between the residual energy of the nodes, the compromised nodes become having less residual energy than the other nodes in a network affected by one type of active attack. This comparison may not conclusive in case of passive attack but mostly in active attack, this comparison is going to be decisive for identifying attackers. The energy of the attacker becomes high or low compared with the neighboring nodes.

VI. CONCLUSION AND FUTURE WORK

This work shows how the throughput, packet drop, and residual energy of the network will vary in the case of with and without attack. This work helps to find out an attack in the network. An attack can be observed if there are changes (increasing or decreasing) in the packet drop, throughput, and residual energy. This work helps to find out the attack in the network more effectively because three parameters (i.e. throughput, packet drop and residual energy) are used one by one to confirm the attack.

To find the attack in the network, selection of one parameter may not help because energy may consume more due to distance, packet size, faulty node, selection of path etc. similarly throughput and packet drop might be affected by some other reasons. In this work security like detecting attack and malicious node in the network. This is one of the security concerns. In future for this another kind of security can be given by giving encryption technique to the network. So that it may give strong security to the network

REFERENCES

1. Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." In Proceedings of the 33rd annual Hawaii international conference on system sciences, pp. 10-pp. IEEE, 2000.
2. Xiangning, Fan, and Song Yulin. "Improvement on LEACH protocol of wireless sensor network." In 2007 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007), pp. 260-264.IEEE,2007.
3. Alsoufi, Delan, Khaled M. Elleithy, Tariq Abuzaghleh, and Ahmad Nassar. "Security in wireless sensor networks-Improving the leap protocol." (2012).
4. Li, Jianpo, Dong Wang, and Yanjiao Wang. "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network." IET Wireless Sensor Systems 8, no. 2 (2017): 68-75.
5. Rasheed, Amar, and Rabi N. Mahapatra. "The three-tier security scheme in wireless sensor networks with mobile sinks." IEEE Transactions on Parallel and Distributed Systems23, no. 5 (2012): 958-965.
6. Misra, Sudip, Ashim Ghosh, and Mohammad S. Obaidat. "Detection of identity-based attacks in wireless sensor networks using signalprints." In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, pp. 35-41. IEEE, 2010.
7. Manishankar, S., P. R. Ranjitha, and T. Manoj Kumar. "Energy efficient data aggregation in sensor network using multiple sink data node." In 2017 International Conference on Communication and Signal Processing (ICCSP), pp. 0448-0452. IEEE, 2017.
8. Anand, Santosh, and R. R. Akarsha. "A Protocol for The Effective Utilization of Energy in Wireless Sensor Network with optimization technique." International Journal of Engineering & Technology 7, no. 3.3 (2018): 93-98.
9. Shanmugham, S. (2009), "Secure Routing in Wireless Sensor Networks", MS EE Scholarly Paper Spring, March 2009.
10. Hassanzadeh, A., Stoleru, R., & Chen, J. (2011), "Efficient flooding in wireless sensor networks secured with neighborhood keys", IEEE Intelligent Systems (pp. 119-126), October 2011.
11. Rolla, P., & Kaur, M. (2016), "Dynamic Forwarding Window Technique against DoS Attack in WSN", International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), Vol. 6, Issue 6, June 2016.
12. Ping, Y., Yafei, H., Yiping, Z., Shiyong, Z., & Zhoulin, D. (2006), "Flooding attack and defence in ad hoc networks", Journal of Systems Engineering and Electronics, Vol. 17, No. 2, 2006.
13. Acharya, A. A., Arpitha, K. M., & Santhosh Kumar, B. J. (2016), "An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET", International Journal of Engineering and Technology (IJET), Vol. 8, No. 2, 2016.
14. Undercoffer, J., Avancha, S., Joshi, A., & Pinkston, J. (2002), "Security for sensor networks", CADIP Research Symposium (pp. 25-26), October 2002.

AUTHORS PROFILE

Nagarjun S a student of Amrita School of Arts & Sciences, Mysuru. He is a BCA graduate from Amrita School of Arts & Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India (2017) and he is currently pursuing his Master of Computer Applications (MCA). His area of research includes Networking and Web Application.

Mr. Santosh Anand has pursued his BE and MTech. His research interest is in Wireless Sensor Network. He I currently working as an Assistant Professor in Amrita School of Arts & Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India.

Mr. Somnath Sinha completed his PhD in Computer Science from the Pacific University, Udaipur, India. He also completed his Master's in Computer Application from the IIEST, West Bengal, India. His research interest is on Security and different types of attack detection in MANET. He is presently working as an Assistant Professor in Amrita School of Arts & Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India.