International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Detection and Prevention of the Sybil Attack in Wireless Sensor Networks using Modified RSSI Scheme

Mandeep Kaur
contactmgrewal@gmail.com
CSE Department
Bhai Gurdas Institute of Engg. & Tech

Mr. Avinash Jethi
Asst Professor
CSE Department
Bhai Gurdas Institute of Engg. & Tech

Abstract: *The nodes in wireless sensor network are not taken care of once deployed to gather information from the hostile environments. This prompts the attackers to steal out the important information by launching various attacks. This paper considers Sybil attack where the attacker impersonates the ID of the genuine node. Earlier the RSSI based scheme has been used to safeguard the WSN against such types of attacks. This paper presents the modified version of the RSSI based scheme which is taken into effect by deploying the high energy sensor nodes. The proposed scheme outperformed the existing scheme in terms of packet delivery ratio and throughput.*

Keywords: *Sybil attack, WSN, RSSI, high energy nodes*

I. INTRODUCTION

With the current advances in micro electro-mechanical system (MEMS) innovation, wireless interchanges, what's more, computerized gadgets, the outline and improvement of minimal effort, low-power, multifunctional sensor nodes that are little in size turned out to be practical. The regularly expanding abilities of these small sensor nodes, which incorporate detecting, information handling, and conveying, empower the acknowledgment of wireless sensor systems (WSNs). WSNs have an extensive variety of uses. As per our vision. WSNs are gradually turning into a necessary piece of our lives. To understand the current and potential applications for WSNs, advanced and greatly effective communication protocols are required. In addition, rather than sending the basic information to the nodes in charge of the combination, sensor nodes utilize their preparing capacities to locally do basic calculations and transmit just the required and halfway prepared information. Subsequently, these properties of WSNs present novel difficulties for the advancement of correspondence protocols. Also these networks are left unattended in the environment after deployment, the changes of the information from getting stolen by the attackers are very high. One of the methods to steal the information is by capturing the ID of the original nodes. This is popularly known as Sybil attack. This paper presents the brief survey of the existing techniques in section II. Then Section III presents the problem in one of the scheme which is modified by the method described in Section IV. Finally, the section V presents the results with the conclusion shown in the last section of the paper.

II. LITERATURE SURVEY

Prameet Kaur and Dr. Sandeep Singh Kang [1] proposed the productive routing LEACH protocol to predict Sybil attack in wireless sensor system. The proposed work utilizes the encryption strategy taking into account the binomial appropriation. In future more attacks can be re-enacted and can check the execution of the proposed work.

Ssu et al. [2] proposed a Sybil attack detection strategy utilizing neighboring data (DSANI). Nodes running this strategy distinguish the Sybil IDs by investigating the neighboring node data. To do this, when a node A suspects there is a Sybil attack, it conveys a Request Reply (RR) message to one of its neighbor B. Thus, node B show a neighbor answer message over its most extreme communication range. The motivation behind a RR message is to look for all its neighbors to send an answer message to the solicitation source A. At that point, node A keeps up a record of node characters of answered nodes to shape a Common Neighbor Set (CNS) of nodes A what's more, B. Along these lines, every node repeats this procedure for every neighbor node. At long last, node A checks how frequently every neighbor identity has showed up in CNS. From this calculation, node characters that show up beneath an edge esteem (θ) are anticipated as Sybil characters. The θ quality is figured as $0.7*|Nc|$, where Nc is the quantity of neighbors. To evade false detection, the previously stated procedure will be repeated by decreasing the communication range until the Sybil personalities fall outside of nodes region. Despite the fact that this technique has demonstrated huge Sybil personalities detection rate, conforming communication range and sending a solicitation message to each neighbor as a major aspect of planning CNS can prompt high communication overhead.
Bin et al. [3] proposed Sybil attack detection strategies based on communication range in WSNs. These techniques work with the

assistance of grapple nodes. These techniques expect that malicious nodes play out the Sybil attack from a settled location in the system. At the point when a node gets the signal message from its neighbors, it computes the polar separation by measuring the polar point. A Sybil attack is identified when the polar separation of various nodes is not exactly an edge esteem. Be that as it may, this technique requires extra equipment setup, for example, stay nodes. From the previously stated writing, it is watched that every strategy its own particular qualities and confinements. A large portion of the strategies are based on ordinary cryptography, utilization of extra equipment setup, for example, stay nodes, and having overwhelming correspondence process. All in all, nodes need to execute the attack detection techniques in conjunction with the application conventions. To this end, a node-driven methodology is required to identify the Sybil attacks productively without extra overheads.

Karupiah et al. [4] proposed an energy efficient Sybil attack detection strategy called Sybil Secure. In this strategy, nodes in the system are gathered into clusters and a cluster head (CH) is chosen from the cluster individuals to start the Sybil attack detection process. CH intermittently conveys an inquiry message requesting that the cluster members respond. Thus, every cluster member responds to the CH request. At that point, CH gathers the data, for example, the IDs of nodes that are not answered inside a response period, node IDs whose points of interest are like past records, and nodes that sent diverse location facilitates. At last, Sybil Secure technique breaks down this accumulation to distinguish Sybil personalities.

Vasudeva et al. [5] proposed a strategy to recognize Sybil attacks on most minimal identity-based clustering calculations. In these calculations, a node with the most minimal identity is chosen as the cluster head for handling the information. In this work, the malicious nodes upset the cluster development process by conveying low identity numbers. Nodes running this technique identify malicious exercises by accepting every neighbor's data.

P. Raghu Vamsi and Krishna Kant [6] proposed a technique for identifying Sybil attack utilizing successive investigation. This technique works in two phases. To start with, it gathers the verifications by watching neighboring node movements. Further, the gathered verifications are combined to give contribution to the second stage. In the second stage, gathered verifications are approved utilizing the successive likelihood proportion test to choose whether the neighbor node is Sybil or genuine. The proposed technique has been assessed utilizing the simulation tool ns-2. Simulation results demonstrate that the proposed technique is powerful in identifying Sybil attacks with low false positive and false negative rates.

Mian Ahmed Jan et. al [7] proposed the concept of high energy nodes which are used to detect the Sybil nodes in the wireless sensor network. Every node is required to transmit a message to these high energy nodes which find the ratio of the received signal strength. Each node has to send messages twice and high energy nodes store two ratios for each nodes. If the difference in the ratios is found to be nearly zero but the Id of the nodes is different than the presence of the Sybil nodes is indicated in the network. Furthermore, these high energy nodes perform the function of relaying the data from the cluster heads to the base station.

III. Research Gap

In [7] the authors have proposed a method to detect the Sybil nodes in the network using the ratio of received signal strength calculated by the high energy nodes in the network. This method relies on the first high energy node to transmit the information about the received signal strength to the nearest second high energy node. However, it can be argued here that a node may have sent a signal to second high energy node which might not be the nearest node w.r.t first high energy node. In simple terms it can be put forward that first high energy node has no information regarding the second-high energy node whom the node is sending the control packet. In such a case the calculation of RSSI ratio would not be possible.

IV. Proposed Work

Initially, each node broadcasts control packets to its two nearest high energy nodes. To the first high energy node the control packet would contain the Id of the second-high energy node and the list of neighbours of the node in the ascending order of the distance. To second high energy node the control packet would only contain the id and residual energy of the node.

When the first high energy node receives the packet, it would calculate signal strength of the received packet, and exchange it with second high energy node whose id is mentioned in the packet. It will now forward the two shortest neighbours out of the list that it received. The second-high energy node will calculate RSSI ratio.

After a certain amount of time, the same operation is performed to calculate a new RSSI ratio using signal strength of received packets from the same node. If the new ratio is equal to the previous ratio and identities of a node in received packets are also different, it means that the node has forged its identities. Each node in the network undergoes a similar operation for identity verification.

The high energy node sends control packet to a base station which makes the final decision on cluster head selection. The base station maintains two queues, one for blacklisted Sybil nodes and one for ordinary sensing nodes along with their shortest neighbour's Ids. If the different ids in the suspected list are having same neighbours occurring repeatedly then the base station would send a control packet to the high energy node.

The procedure of Sybil attack detection is repeated at the start of each round before cluster formation and cluster head selection. Once a Sybil node is detected, it is blacklisted to withhold its participation in cluster head selection.

V. Results

The proposed scheme as well as the existing scheme [7] was implemented on NS 2.35 which is open source simulator. The simulation parameters used in the work are defined below:

Table I: Simulation Parameters

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Parameter	Value
Channel	Wireless
Propagation Model	Two Ray Ground
Network Interface	WirelessPhy
Number of nodes	101
Mac	802.11
Antenna	Omni Directional
Network Area	1400m * 1400m
Queue	Drop Tail
Energy Model	Radio Dissipation Energy Model

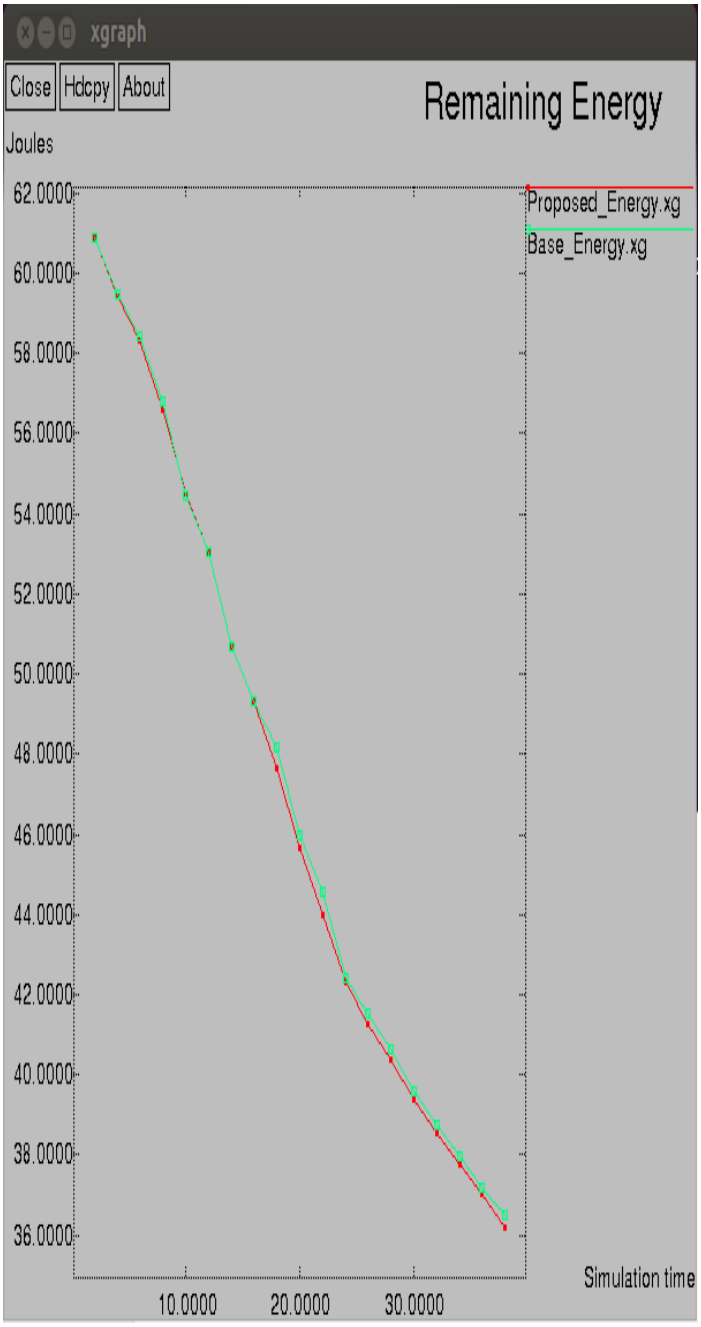

Figure 1. Remaining Energy Comparison

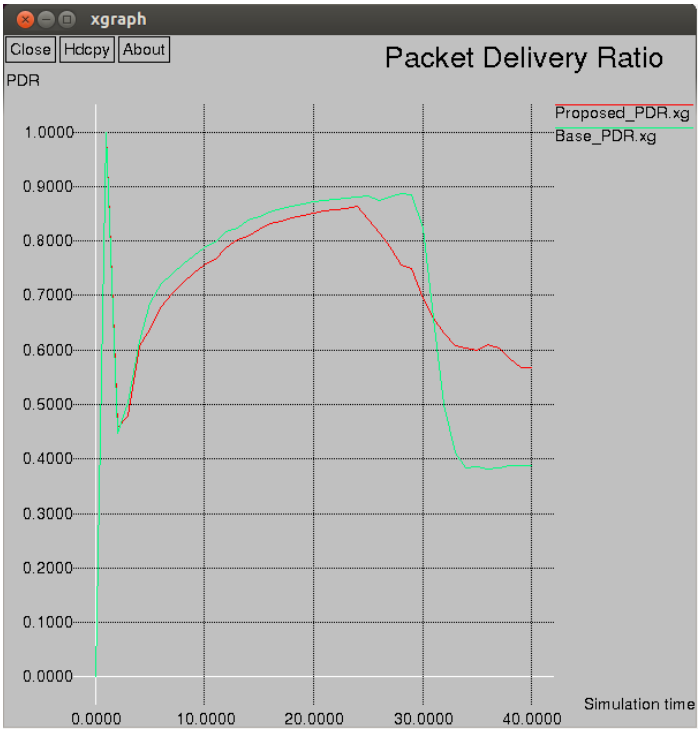

Figure 2. PDR Comparison

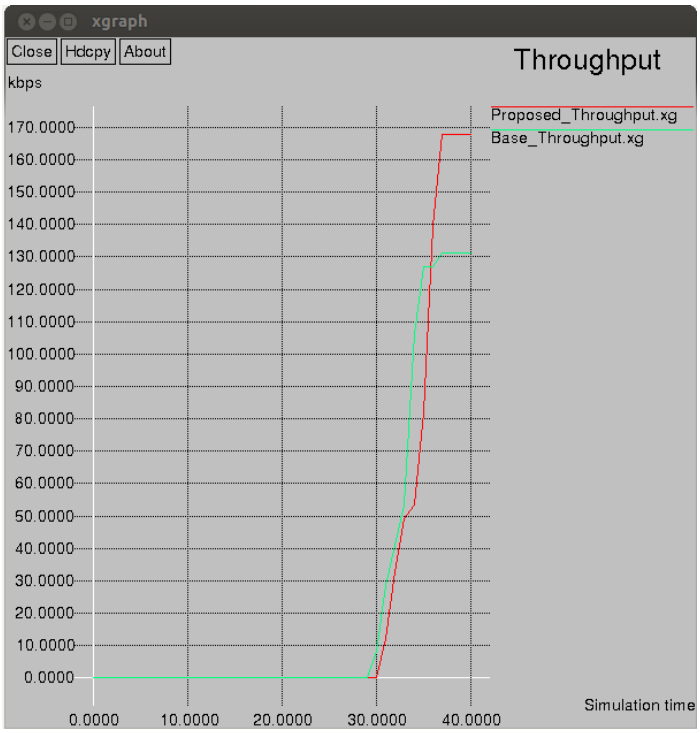

Figure 3. Throughput

VI. Conclusion and Future Work

The performance of the network was analyzed on the basis of packet delivery ratio, throughput and remaining energy of the network. The packet delivery ratio as well as throughput showed better performance than the existing scheme. The values for packet delivery ratio were found to be at 58 percent while the same values for the existing scheme were 39 percent. Similarly, the throughput values for the existing scheme were 131 kbps and for the proposed scheme these values were 169 kbps. Since the proposed scheme gave focus only on the better detection of the Sybil nodes, so the values for the remaining energy parameter has been found to be same for both the schemes.

In future, the same scheme can be extended to perform the detection of the Sybil nodes in more energy efficient way. Also, the proposed scheme has taken one hop communication between the high energy nodes and the base station, and also between the ordinary nodes and the high energy nodes, the same thing can be extended to the multi hop for better energy utilization as well as better packet delivery ratio of the network.

VII. REFERENCES

[i] Prameet Kaur and Dr. Sandeep Singh Kang, " Optimized secure routing protocol to prevent Sybil attack in wireless sensor networks " in International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013

[ii] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting Sybil attacks in wireless sensor networks using neighboring information," Computer Networks, vol. 53, no. 18, pp. 3042- 3056, 2009.

[iii] B. Tian, Y. Yao, L. Shi, S. Shao, Z. Liu, and C. Xu, "A novel Sybil attack detection scheme for wire-less sensor network," in 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT), pp. 294-297, IEEE, 2013.

[iv] M. A. B. Karuppiah and A. R. Prakash, "Sybil secure: An energy efficient sybil attack detection technique in wireless sensor network," International Journal of Information, vol. 4, no. 3, 2014.

[v] A. Vasudeva and M. Sood, "Sybil attack on lowest id clustering algorithm in the mobile ad hoc network," International Journal of Network Security & Its Applications (IJNSA), vol. 4, no. 5, 2012.

[vi] P. Raghu Vamsi and Krishna Kant, " Detecting sybil attacks in wireless sensor networks using sequential analysis" in international journal on smart sensing and intelligent systems vol. 9, no. 2, june 2016

[vii] Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network", 2015 IEEE Trustcom/ BigDataSE/ ISPA.