Sybil Attack on Aggregated Data in Wireless Sensor Networks

Shilpy Ghai[1], Prof. V.K.Katiyar[2]
[1]*M.M.Engineering College, Maharishi Markandeshwar University, Mullana, Haryana, India (Research Scholar)* [2]*M.M.Engineering College, Maharishi Markandeshwar University, Mullana, Haryana, India (Professor, CSE Department)*

Abstract- In both academia and industry field, Wireless Sensor Networks (WSNs) is an emerging and promising field. The use of such kind of networks is extended due to their unique properties, such as self-organization and ease of deployment. However, there are still some technical challenges, such as energy efficiency which depend on the number of packet loss, throughput of the network, delay time and so on. We have used data aggregation to get the required result. Data aggregation will reduce the data redundancy which will help in energy efficient data transmission. We have made new data aggregation technique by hybridizing two data aggregation techniques which are Dynamically Balanced Spanning Tree (DBST) and Redundancy Eliminated Data Dissemination (REDD).There are so many attacks which affect the security of the network. Sybil attack is one of them. In our paper, we have applied sybil attack on the aggregated data.

Keywords- Wireless Sensor Network, Data aggregation, sensor nodes, attacks.

I. INTRODUCTION

A Wireless Sensor Network consists of a large number of sensors of physically small devices, and is outfitted with the capability of data processing, sensing the physical environment, and communicating wirelessly with other sensors. Commonly, we assume that each sensor in a wireless sensor network has certain constraints with respect to its energy source, power, memory, and computational capabilities (1).

WSN used tiny, inexpensive sensor nodes with several distinguishing characteristics: limited and specific monitoring and sensing functions are performed by them and they have very low processing power and radio ranges, by which consumption of energy will be very low. WSN is form by a several such wireless sensors in a region self-organize. In agriculture and livestock information based on sensed data can be used, even in providing security at home or in public places. To provide adequate security capabilities is a key requirement from both the technological and commercial point of view. Offering pervasive services is essential for user acceptance for fulfilling privacy and security requirements in an appropriate architecture for WSNs (2). Scalability, security, reliability, self-healing and robustness are the five key features need to be considered when developing WSN solutions.

The field of wireless sensor networks has become a focus of exhausted research in recent years and addressed various theoretical and practical questions. Result of the possibility of pairing these devices with their surroundings has drawn a lot of attention. Well beyond their direct use, such as surveillance and environmental monitoring, WSNs can help us to follow one of the ultimate goals in information technology, namely ambient intelligence (3). The information about the physical world around us and the flexibility to have them integrated deeply within building material, fabrics, and embedded in inaccessible or hostile locations in the real world operating scenarios is provided us with the small size and wireless communication capability of sensor nodes in a WSN. Automated intelligent systems is developed by using wireless sensor networks that can contribute with each other to exchange information respecting their internal states and the conditions of the physical environment around them, prevent disasters with better efficiency and robustness without any interference by human and services is provided to users (3).

A. Sensor Network Challenges

A wide variety of applications are used by Wireless Sensor Network and to force these applications in real world environments we need more client protocols and algorithms. While designing a new protocol or algorithm we face some challenges which are need to be clearly understood (4). These challenges are summarized below:

• *Security:* Encompassing the characteristics of authentication, integrity, privacy and non repudiation security is broadly used name. As more the dependency on the information provided by the networks has been increased the risk of secure transmission of information over the network has increased. Several cryptographic, steganographic and other techniques are used for the secure transmission of various types of information over networks,.

• *Physical resource constraint*: The most important constraint is set on sensor network is the limited battery power. The effective lifetime of a sensor node is directly determined by its

power supply. Hence by power supply the sensor network lifetime is also determined. The main design issue of a protocol is energy consumption. Anoth0er constraint that affects the amount of data that can be stored in individual sensor nodes is limited computational power and memory size. So the protocol should be simple and light-weighted. Communication delay in sensor network can be high due to limited communication channel shared by all nodes within each other's transmission range.

• *Fault-Tolerance*: In a hostile environment, a sensor node may fail due to physical damage or lack of energy (power). If some nodes fail, the protocols that are working upon must contain these changes in the network. As an example, for routing or aggregation protocol, they must find suitable paths or aggregation point in case of these kinds of failures.

• ***Scalability***: Most of the applications are needed; the number of sensor nodes redistribute must be in order of hundreds, thousands or more. The protocols must extensible enough to respond and operate with such large number of sensor nodes.

• *Quality of Service*: From the moment it is sensed data should be delivered within a certain period of time, some real time sensor applications are very time critical otherwise the data will be unusable. So for some applications this must be a QOS parameter.

• *Unattended operation*: Sensor networks are arranged once in number of application, and after arrangement have no human interference. The nodes themselves are responsible for reconfiguration in case there is any changes.

B. Attacks in Wireless Sensor Networks

Denial of service (DoS): DoS is produced by not planned failure of nodes or malicious action. It tries to disable the resources available to the victim node by sending extra unnecessary packets. At different layers, the DoS attacks could be Jamming, tampering, collision, misdirection, flooding etc.

*Attacks on information in transit***:** Sensors monitor the changes of specific parameters in case of a sensor network, and address about it to the sink according to the requirement. During transmission the report can be changed or disappeared.

*Sybil attack***:** Sybil attack is that in which a node produces the identities of more than one node.

Blackhole/sinkhole Attack: In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Attacker tries to insert the malicious node into the network to do anything with the packets passing between them.

*Hello Flood Attack***:** In this attack, **Hello** packets are used to assure the sensors in WSN. Within the WSN these packets are delivered in a large area. The sensors are thus convinced that the attacker is their neighbour.

*Wormhole Attack***:** In this attack, at one location in the network attacker records the packets and tunnels those to another location. We can do bits tunnelling or its retransmission could be done selectively.

C. Data Aggregation

Data Aggregation is the technique in which data is gather and then aggregate that data in an efficient manner which will reduces redundancy so that network lifetime is enhanced. The data accuracy will increase by arrangement of large number of sensors over sensing area. The sensors used in the nearby region sense the same phenomena which lead to produce lot of duplicate data. This will cause redundancy and leads to more bandwidth and energy consumption. Data De- distribution means removing duplicate data to reduce the redundancy. To perform De-duplication data aggregation techniques are used (5). In data aggregation sensor data is collected by sensor nodes are aggregated by using some data aggregation algorithms and then aggregated data is forwarded towards base station.

For data aggregation strategies, number of approaches are available which are In-network aggregation, with size reduction, without size reduction, Tree-based approach, and cluster-Based approach. *We will use the hybrid techniques (combinations of DBST and REDD) for data aggregations.* Dynamically Balanced Spanning Tree (DBST) (6) which provides dynamic structure of tree to solve hotspot problem and improve energy conservation.

Redundancy Eliminated Data Dissemination (REDD) (7) algorithm makes use of context aware system for validation and correlation coefficient is used to eliminate redundancy from valid data.

D. Sybil Attack

Sybil Attack is named after the subject of the book Sybil, a case study of a woman diagnosed with multiple fake identities. These fake identities are known as Sybil nodes. The Sybil nodes can vote out the honest nodes in the system. Usually, peer to peer systems are vulnerable to Sybil attack. Examples of vulnerable systems include vehicular Ad hoc Network, Distributed Storage Applications in Peer to Peer Systems, Routing in a Distributed Peer to Peer System.

II. RELATED WORK

In 2015 Udaya Suriya Rajkumar, et al**.** (153) have done a survey on Sybil attack and proposed a new approach i.e., Compare and Match (CAM) approach to verify the position so that Sybil attacks can be prevented. Till now by number of researchers it have been identified that there are large number

of attacks in WSN out of which the Sybil attack is one of the harmful attacks against sensor network. Major information has been lost by this kind of attacks and hence misinterpretation is created in the network. In this scheme a node can trust the pretend node and it start sharing its information. A node's security is affected and information is lost due to this activity. By using network simulator under various conditions, by measuring throughput, end to end delay and packet delivery ration the practical analysis of this work has been done.

In 2015 Itesh Sharma, et al. (154) have done this survey in order to design more efficient and practical Sybil defences, The Sybil attack is an attack where in peer-to-peer networks a reputation system is subverted by a considerable number of forging identities. By illicitly infusing false or biased information via the pseudonymous identities, an adversary can mislead a system into making wrong decisions. The research on the Sybil defense technique has experienced four phases: (1) traditional security key-based approaches, (2) specific peer-to-peer system feature-based solutions, (3) social network-based methods, and (4) social community-based techniques. They have presented some Sybil defense schemes, including social graph based Sybil detection, behaviour classification based Sybil detection, and mobile Sybil detection with the comprehensive comparisons. Security and performance analysis shows that by their proposed neighbor similarity trust Sybil attack can be minimized.

In 2015 Udaya Suriya Raj Kumar Dhamodharan, et al. (155) has proposed a combined Compare and match-Position verification method (CAM-PVM) with Message authentication and passing (MAP) for detecting then eliminating and also preventing the entry of Sybil nodes in the network. For securing network protection wireless sensor networks are highly crucial. Highly critical attacks of various kinds have been documented in wireless sensor network by number of researchers. The Sybil attack is a heavy destructive attack against the sensor network which already have been concluded and seen from previous paper. How it can actually effect the WSN is also have been examined in previous papers by different researchers. By analyzing the neighbours the node identifies are verified for this there is only scheme which is Random Password Comparison. With the objective of resolving this problem a survey was done on a Sybil attack and from that the author have proposed a scheme which assure the security for wireless sensor network, to deal with attacks of these kinds in unicasting and multicasting.

In 2016 Ayan kumar das, et al. (157) proposed a new routing technique to prevent from both external threats and internal threats like hello flooding, eavesdropping and wormhole attack. In the approach used in this paper to reduce the energy drainage is one way hash chain. Energy can also be saved by Level based event driven clustering. The simulation results of this paper show that even when the cluster based wireless sensor network is under attack the proposed scheme can extends the lifetime of network.

In 2016 P. Raghu vamsi, et al. (158) analysed that WSNs suffer from many security attacks when use either in remote or hostile environments. Have seen in previous papers that the Sybil attack is one of the severe attacks in which malicious nodes report false identities and location information such that the remaining nodes believe that many nodes exist in their vicinity. In this paper they have proposed a method for detecting Sybil attack using sequential analysis. This method works in two stages. First, by observing neighbouring node activities it collects the evidences than that collected evidences are combined to provide input to the second stage. In this stage, to decide whether the neighbour node is Sybil or benign that collected evidences are confirmed using the sequential probability ratio test. By using the network simulator ns-2, the proposed method has been evaluated. This paper simulation results show that the proposed method is very powerful in detecting Sybil attacks with very low false positive and false negative rates.

In 2016 Rupesh Gunturu, et al. (159) reviewed the different defence mechanisms used to reduce Sybil attacks and also reviewed the Sybil attack in social networks, which has the ability to compromise the whole distributed network. To compromise the whole network the malicious user demand for multiple identities in the Sybil attack. In voting applications, bad-mouth an opinion, access resources or to break the trust mechanism behind a Peer to peer network the Sybil attacks can be used to change the overall ranking.

In 2016 Brian Neil Levine, et al. (160) have given a overview of work related to analyzing or solving the Sybil attack controls many different identities categorized 90 papers that mention either the Sybil attack or pseudo spoofing (an earlier term for the use of multiple false identities) into eleven categories and described each approach. They have also demonstrated the breadth of applications that are subject to the attack.

III. PROPOSED WORK

ALGORITHM:

This work deals with the hybridization of the DBST and REDD algorithms for the data aggregation in Wireless sensor networks (15).

1. First, we have implemented DBST technique, in which cluster formation takes place and this deals with the hierarchical manner in which we will get an ordered manner of our network.
2. Each cluster is having number of nodes and each node will have different energies.

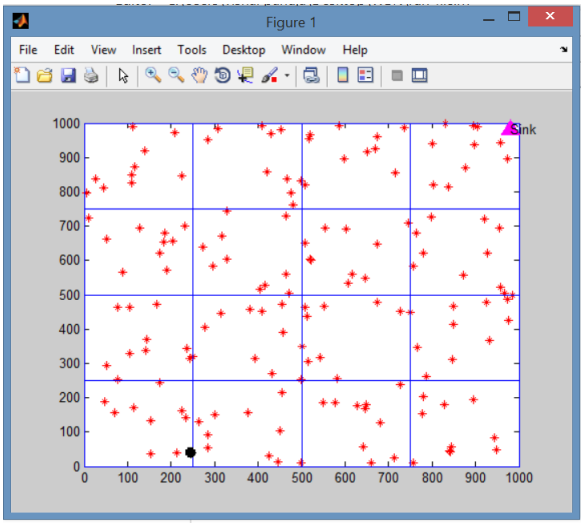

Fig.1: Cluster formation

3. Each cluster will have one cluster head because instead of harvesting all energies of the node, Cluster head will communicate on behalf of each cluster for the conservation of energy and it will communicate with the sink node.

4. Then those cluster heads will be having tree structure as mentioned in the REDD structure which deals with the tree data structure.

5. In tree data structure, there is root node and leaf node and route will be performed from leaf node to root node and the root node is that cluster node which is having high residual energy than other cluster head nodes and those contains data in the form of packets which will be transferred to the root node.

6. The route will be performed with the use of the link weight [16].

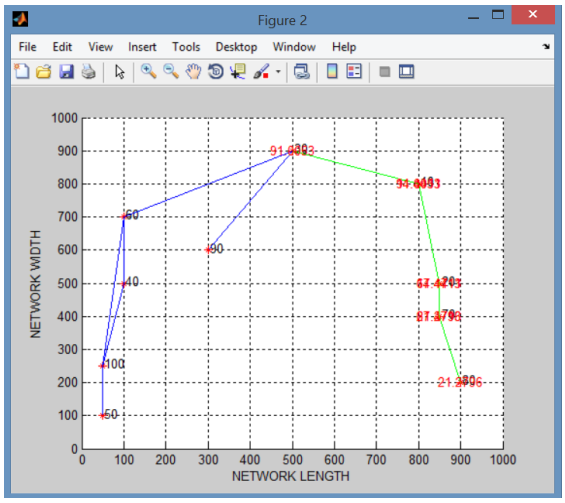

Fig.2 selected route

7. The nodes are showing the selected route through which the packets are sending to the root nodes which is performing routing.

8. The below figure shows the Sybil attack which shows the multiple copies of the original node in the yellow color which will increase the load in the network. This will decrease the lifespan of the network. The Sybil attack is the routing attack due to which the packets will be dropped and it will increase the energy consumption of the network.

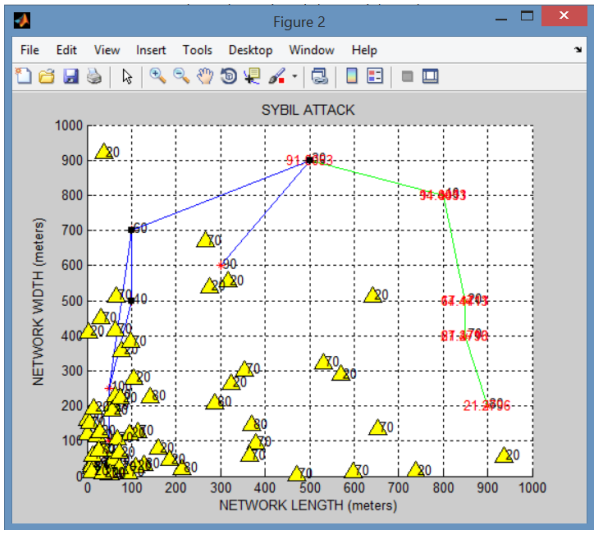

Fig.3 Sybil Attack

IV. CONCLUSIONS

This paper provides brief description of various data aggregation protocols and attacks in wireless sensor networks. This paper also gives a proposed data aggregation technique to reduce redundancy to reduce energy consumption. This hybrid technique will provide better energy utilization. Then we have applied Sybil attack on the aggregated data. Further, we will work upon an optimized algorithm to protect the wireless sensor network from sybil attack and to make it energy efficient and secure. We will find out some parameters like loss of packets, throughput, end delay etc.

V. REFERENCES

[1]. Neha, Dua; R & Mathur, V. Wireless Sensor Networks: Architecture, Protocols, Simulator Tool. International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vol 2, Issue 5, pp. 229-233.

[2]. Sohraby, K.; Minoli, D. and Znati, T.F; Wireless sensor networks: technology, protocols, and applications, 2007, Wiley-Blackwell.

[3]. Chong, C.-Y. and S.P. Kumar, Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE, 2003, pp. 1247-1256.

[4]. Chong, C & Srikanta, P. (2003). Sensor Networks :Evolution, opportunities, and Challenges. Proceedings of the IEEE, Vol.91, no.8, pp. 1247-1255.

[5]. Avokh, Avid ; Patil, Ghasem Mirjalily. Dynamic Balanced Spanning Tree (DBST) for Data Aggregation in Wireless Sensor Networks. 5th International Symposium on Telecommunications, IST2010, 978-1-4244-8185-9/10 , 2010 IEEE.

[6]. Ramachandran, Sumalatha; Gopi, Aswin Kumar; Elumalai, Giridara Varma ; Chellapa, Murugesan. REDD: Redundancy Eliminated Data Dissemination in Cluster Based Mobile Sinks. ICRTIT 2011, 978-1-4577-0590-8/11, 2011 IEEE.

[7]. Gagarin, A.; Hussain, S. and Yang, L.T. Distributed hierarchical search for balanced energy consumption routing spanning trees in Wireless Sensor Networks. J. Parallel Distrib. Comput, 2010, Vol. 70, no. 9, pp. 975-982.

[8]. Suriya, Udaya; Kumar, Raj; Dhamodharan and Vayanaperumal, Rajamani. Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method. The Scientific World Journal, 2015, Vol. 2015, pp. 1-7.

[9]. kumar das, Ayan; chaki, rituparna; dey, kashi nath. Secure energy efficient routing protocol for wireless sensor network. Foundations of computing and decision sciences, 2016, Vol. 41.

[10]. Vamsi, P. Raghu and kant, Krishna. Detecting sybil attacks in wireless sensor networks using sequential analysis. International

[11]. Gunturu, Rupesh. Survey of Sybil Attacks in Social Networks.

[12]. Levine, Brian Neil; Shields, Clay; Boris Margolin, N. A Survey of Solutions to the Sybil Attack.

[13]. Parameswari, K.; Raseen; M.Mohamed. Aggregating Secure Data In Wireless Sensor Networks. International Conference on Current Trends in Engineering and Technology, ICCTET'13, 2013, pp. 381-383.

[14]. Tao Du, Shouning Qu, Kaiqiang Liu, Jinwen Xu, Yinghua Cao. An efficient data aggregation algorithm for WSNs based on dynamic message list. The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016), 2016, Vol. 83, pp. 98-106.

[15]. ghai shilpy, katiyar vk ," Data Aggregation to improve Energy Efficiency in Wireless Sensor Networks" IJIRIS, oct 2016, pp. 9-12.

[16]. FU,Ziang et al," An Energy Balanced Algorithm of LEACH Protocol in WSN" IJCSI, vol 10, issue 1, jan 2013