www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21465-21467
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.45

Efficient Defense Mechanism against Sybil Attack in Wireless Sensor Network

***Priyanka*[1]**
Department of Computer and Science Engineering[1]
R.N. College of Engineering and Management,
Maharshi Dayanand University,
Rohtak, Haryana

Abstract: Sensor network consists of tiny sensors and actuators with general purpose computing elements to cooperatively monitor physical or environmental conditions, such as temperature, pressure, etc. Wireless Sensor Networks are uniquely characterized by properties like limited power they can harvest or store, dynamic network topology, large scale of deployment.

Keywords: Wireless sensor network Cluster-based routing protocols, Sybil, malicious cluster head.

1. Introduction

Wireless sensor network is a collection of nodes (sensors) organized into a cooperative network [1]. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omnidirectional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. Wireless Sensor Networks are characterized by:

- Limited power they can harvest or store.
- Ability to cope with node failures.
- Heterogeneity of nodes.
- Large scale of deployment.
- Mobility of nodes.

2. CLUSTERING IN WSN

Clustering is an important mechanism in large multi-hop wireless sensor networks for obtaining scalability, reducing energy consumption and achieving better network performance. Most of the research in this area has focused on energy-efficient solutions, but has not thoroughly analysed the network performance, e.g. in terms of data collection rate and time. It is evident that by organizing the sensor nodes in groups i.e., clusters of nodes, we can reap significant network performance gains LEACH is the first network protocol that uses hierarchical routing for wireless sensor networks to increase the life time of network. All the nodes in a network organize themselves into local clusters, with one node acting as the cluster-head. All non-cluster-head nodes transmit their data to the cluster head, while the cluster-head node receive data from all the cluster members, perform signal processing functions on the data (e.g., data aggregation), and transmit data to the remote base station. Therefore, being a cluster-head node is much more energy-intensive than being a non-cluster-head node.

3. Sybil attack:

The Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. We refer to a malicious device's additional identities as Sybil nodes. We propose three orthogonal dimensions: direct vs. indirect communication, fabricated vs. stolen identities, and simultaneity.

DOI: 10.18535/ijecs/v6i5.45

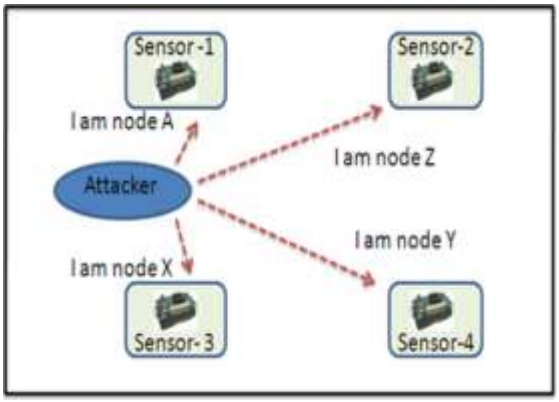

Fig: Sybil Attack

4. RELATED WORK

J. Dalfiah [1] et al proposed an energy-efficient integrated Intrusion Detection System (IDS) to detect network layer Sybil attack. Their scheme spots out accurately and purges out the Sybil node which may falsely behave as a genuine node. The experimental results showed that the critical factor in WSN, energy is conserved more efficiently by the proposed scheme than the existing alternative methods. Also, accurate detection of the malicious node is possible spending relatively less energy. T. G. Dhanalakshmi[2] et al explains the Securing Grid protection in Wireless Sensor Grids (wireless sensor networks) several attacks that have been recognized in wireless sensor network till now by the researchers and still it's increasingly becomes critical. Sybil attack is one of the harmful attacks against sensor Grid where a number of appropriate individualities and forged individualities are used to get an inappropriate entry into the network. Essentially a Sybil attack means a system which pretends its individuality like further nodes. In this scenario a system can trust the reclose system and it start sharing its data. Due to this activity a node's safety is affected and data is lost. In this paper, a survey has been done by the authors on Sybil attack and projected a mutual RAI - Relate and Identify Tactic and LVT Location Verification technique to avoid these attacks. M. S. Khalil [3] et al proposed E-BIOSARP that enhances the BIOSARP with random key encryption and decryption mechanism. They have presented the design, pseudo code and the simulation results to prove the efficiency of E-BIOSARP for WSN. Network simulator 2 (NS2) has been utilized to perform the analysis. The result showed that proposed EBIOSARP can efficiently protect WSN from spoofed, altered or replayed routing information attacks, selective forwarding, acknowledgement spoofing, Sybil attack and hello flood attack.

X. Zhenghong [4] et al describe the simulation results which show that the proposed protocol can detect and defend against several sophisticated routing attacks such as Sybil, Wormhole, Selective Forwarding and Hello flood attacks.

R. Vamsi [5]suggested a lightweight Sybil attack detection framework (LSDF). This framework has two components: first, evidence collection; second, evidence validation. Every node in the network collects the evidences by observing the activities of neighboring nodes. These evidences are validated by running sequential hypothesis test to decide whether neighboring node is a benign node or Sybil node. With extensive simulations, it was revealed that the LSDF can detect Sybil activity accurately with few evidences.

I. Makhdoom [6] et al have carried out a detailed review and analysis of various defenses proposed against Sybil Attack.

The authors have identified their strengths and weaknesses and also propose a novel One Way Code Attestation Protocol (OWCAP) for wireless sensors networks, which is an economical and a secure code attestation scheme that protects not only against Sybil Attack but also against majority of the insider attacks.

Y. Sun [7] et al have proposed a regional statistics detection scheme (RSDs) against sybil attacks, which is an effective solution to three key issues: firstly, the authors have addressed the sybil attack by a RSSI-based distributed detection mechanism, secondly, their protocol can prevented the network from a large number of nodes failure caused by sybil attacks, Thirdly, the RSDs has been verified can maintain a high detection probability with low system overhead by implement experiments. Finally, the authors run their protocol in a prototype detection system with 32 nodes that the experiment result confirmed its high efficiency.

5. THE PROPOSED MISUSE DETECTION SYSTEM

In the proposed work we tend to modify the centralized IDS scheme which is based on the misuse detection [5] to detect the malicious cluster head which has the intention of causing the Sybil attack in the wireless sensor network. The proposed scheme works as descry Any kind of malicious activity in the network will be detected by the base station in the network.

- Initially the nodes will be deployed in the network.
- The cluster head will be selected among the nodes on the basis of the residual energy. This is the

remaining amount of the energy in the nodes. The node with highest energy will be selected as the cluster head.

- The sybil node present in the cluster may exhibit the Id of the cluster head and send hello messages to the nodes asking them to join its cluster.
- The nodes receiving the messages will join the respective cluster heads.
- After formation of the clusters in the network, the cluster heads will send the control packet to the Base Station using single hop communication. the control packet will contain the ID and location of the cluster head as well as the ID and location of its members.
- After receiving the control packets the Base Station will detect the malicious cluster head on the basis of the following condition.
- Sybil node has compromised the ID of the cluster head of the same cluster in which it is located.
- Base Station will check if in any cluster it has received control packet with multiple nodes having the same ID.
- The base station will store the ID and location of both the suspects. The base station will send a message to the nodes in the cluster to select the cluster head again.
- The sybil node will again exhibit the Id of the new cluster head.
- The newly selected cluster head will again have to send control packet to the base station which contain the ID and location of the cluster head as well as the ID and location of its members.
- The base station will again receive multiple nodes with same ID.
- The base station will compare the Id and location received in the new control message with the id and location received previously.
- Since the location of the sybil node will be same, the base station will detect that it has received two control packets from the two different cluster heads but they are located at same position in the cluster.
- The base station will inform the member nodes about the location of the sybil node so that they do not communicate with it.
- The base station will now select cluster head from the list of members received in the control packet.

6. CONCLUSION

In WSNs, two of the most important concerns is the vulnerability to many types of security threats. In order to address the above point, we have proposed in this paper an work in which we tend to modify the centralized IDS scheme which is based on the misuse detection to detect the malicious cluster head which has the intention of causing the Sybil attack in the wireless sensor network. Literature work confirm the effectiveness of our modified IDS in terms of the correct detection of all existing attacks. As a future work, we will extend our IDS, to be able to detect other routing attacks such as Hello Flood attacks.

REFERENCES

1. A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, A. S.K. Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks" , 3rd International Conference onEco-friendly Computing and Communication Systems (ICECCS) 2014 IEEE.

2. T. G. Dhanalakshmi, N. Bharathi, M. Monisha, "Safety concerns of Sybil attack in WSN" , International Conference on Science Engineering and Management Research (ICSEMR), 2014 IEEE.

3. K. Saleem, M. S. Khalil, N. Fisal, A. A. Ahmed, " Efficient Random Key Based Encryption System for Data Packet Confidentiality in WSNs, " 12th IEEE International Conference onTrust, Security and Privacy in Computing and Communications (TrustCom), 2013.

4. X. Zhenghong, C. Zhigang, "A Secure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Networks, " International Forum on Information Technology and Applications (IFITA), 2010 (Volume:1) IEEE.

5. P. R. Vamsi, K. Kant, "A lightweight Sybil attack detection framework for Wireless Sensor Networks" , Seventh International Conference on Contemporary Computing (IC3), 2014. IEEE

6. I. Makhdoom, M. Afzal, I. Rashid, "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks" , National Software Engineering Conference (NSEC), 2014. IEEE

7.M. Li, Y. Xiong, X. Wu, X. Zhou, Y. Sun, S. Chen, X. Zhu, "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs" , 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013. IEEE.