
Prabhjot Kaur1, Aayushi Chada2, Sandeep Singh3
Universal Group of Institutes Lalru, Punjab, India1,2
Guru Nanak Dev University Amritsar, Punjab, India3

Abstract:
In spite of their vitality proficiency, the vast majority of WSN's group based directing conventions are vulnerable against security dangers. In this paper, a new misuse detection system is proposed to the malicious cluster head which has the intention of causing the Sybil attack in the wireless sensor network. The proposed misuse detection technique is simple and secure; it is thus suitable for sensor

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

I. INTRODUCTION
A wireless sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. WSN is a very large array of diverse sensor nodes that are interconnected by a communication network. The sensing data are shared between the sensor nodes and are used as input for a distributed estimation system. The fundamental objectives for WSN are reliability, accuracy, flexibility, cost effectiveness, and ease of deployment. WSN is made up of individual multifunctional sensor nodes. Organization of large multi-hop wireless networks into clusters is essential for achieving basic network performance. In wireless sensor networks (WSN), the clustering is primarily characterized by data aggregation by each cluster head, which significantly reduces the traffic cost. The hierarchical model requires two main methods: Periodic selection of cluster heads (CHs) and Assignment of each node to one or multiple clusters.

II. 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 analyzed 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.

III. SYBIL ATTACK
Sybil node is the process of creating two or more duplicate nodes with similar identity i.e. same node id as shown in Fig. 1. Particularly, wireless sensor networks are more prone to Sybil attack because of the open and broadcast communication medium and the same frequency is being shared among all nodes. In Sybil attack, attacker makes multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. So the base station cannot distinguish the legitimate and the forged node. This confuses the base station and other nodes and the network performance degrades.

IV. 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 E-BIOSARP 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. Makhdooom [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.

V. 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 described below:

- 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.

VI. 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
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.


