OVERVIEW OF SYBIL ATTACK: ANALYSIS AND DETECTION

Sukhpreet Kaur\textsuperscript{a},\textsuperscript{*}, Dr. Parminder Singh\textsuperscript{b}

\textsuperscript{a} MTech Student, princypreet@yahoo.co.in, Chandigarh Engineering College, Landran, Punjab, India
\textsuperscript{b} Assistant Professor, singh.parminder06@gmail.com, Chandigarh Engineering College, Landran, Punjab, India

\textbf{ABSTRACT:}

This paper defines the Sybil attack and comparative analysis with different Attacks; among these attacks, Sybil Attack is dangerous attack. This malicious node access the information from the network region of wireless sensor network and that node either modifies or dropping the packets in the network region known as Sybil Attack. The current study addresses two major problems that every network will be facing i.e. Trust and Authentication. The security protocol establishes the trust in the network but instead of these protocols we enable the trust and authentication by Cluster Head Node; this Cluster Head node provides rules and regulation, on the basis of the rules and regulations we authenticate the nodes and detecting Sybil Attack.

\textit{Keywords:} Sensor, Cluster Head, Routing Table, Sybil, Network Region.

\textbf{INTRODUCTION}

Traditional Ad hoc networks consist of network sizes on the order of 10s, sensor networks are expected to scale to sizes of 1000s. Sensor nodes are typically immobile, meaning that the mechanisms used in traditional ad hoc network protocols to deal with mobility may be unnecessary and overweight. Since nodes may be deployed in harsh environmental conditions, unexpected node failure may be common [8]. Incorporating these unique features of sensor networks into protocol design is important in order to efficiently utilize the limited resources of the network. The trust based relationship is the basis for the security framework in the integrated networks against the connectivity and mobility-related attacks in addition to routing related threats.
(a) Sybil Attack

In a Sybil attack, a malicious node pretends the identity of several nodes, by doing so undermining the effectiveness of fault-tolerance schemes, such as the redundancy of many routing protocols. Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. By using the Sybil attack, an adversary can act in more than one place at the same time [5].

(b) Security Problems

Security problem may happen at network layer and include: data integrity attacks, by accessing, modifying, or injecting traffic; denial-of-service attacks; flow-disruption attacks, by delaying, dropping, or corrupting data passing through, but leaving routing traffic unmodified; passive
eavesdropping; resource depletion attacks, by sending data with the objective of congesting a network or draining batteries; signaling attacks, by injecting erroneous routing information to divert network traffic, or making routing, inefficient; and stolen device attacks.

(c) Modification in Sybil Attack

While acting as an intermediary node and receiving the data packet from a source node, a malicious sensor node intentionally modifies, drops, or injects data packets before forwarding to the next hop.

II. PROBLEM DEFINITION

Sybil attack is defined as an attack by a malicious device adopting multiple identities illegitimately and the additional identities are known as Sybil nodes. The Sybil attack can occur in a WSN since it operates without a central authority which can verify the identities of each communicating entity [9]. Because each entity is only aware of others through messages over a communication channel, a Sybil attacker may take different identities during transmission of message to the legitimate node. To defend against Sybil attack it is required to have the knowledge of its different forms.

III. PLANNING OF WORK:

The following steps has been identifies the Sybil Attack.

1. Group of mobile nodes are taken.
2. One of the nodes randomly is taken as observer.
3. The observer node sends HELLO packets to all the other nodes.
4. The node with minimum packet drop is taken as right observer.
5. The node having the maximum packets drop is suspected to be the Sybil node.
6. The other nodes send their identification to the new observer (right observer).
7. The observer transmits data to all other nodes for a particular time interval to capture the behavior of other nodes.
IV. CONCLUSION

Security is Integrated in the Multi-Hop Wireless Sensor Networks and if the Multi-Hop routing is corrupted by the malicious Node then Sybil Attack performing on the Network Region. In the process of finding malicious node, it is necessary to executes the rules of proposed approach enforce the other node to follow the rules. As infrastructure scheme it was easy to detect the misbehavior node that neglects the security rules.
REFERENCES


