INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 1, Issue 1, OCTOBER 2015.

OVERVIEW OF SYBIL ATTACK: ANALYSIS AND DETECTION

Sukhpreet Kaur[a,*],Dr.Parminder Singh[b]

[a] *MTech Student, princy_preet@yahoo.co.in,Chandigarh Engineering College,Landran,Punjab,India*
[b] *Assistant Professor, singh.parminder06@gmail.com,Chandigarh Engineering College,Landran,Punjab,India*

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.

Keywords: Sensor, Cluster Head, Routing Table, Sybil, Network Region.

INTRODUCTION

Traditional Ad hoc networks consist of network sizes on the order of 10s, sensor networks areexpected to scale to sizes of 1000s. Sensor nodes are typically immobile, meaning that the mechanisms used in traditional ad hocnetwork 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.

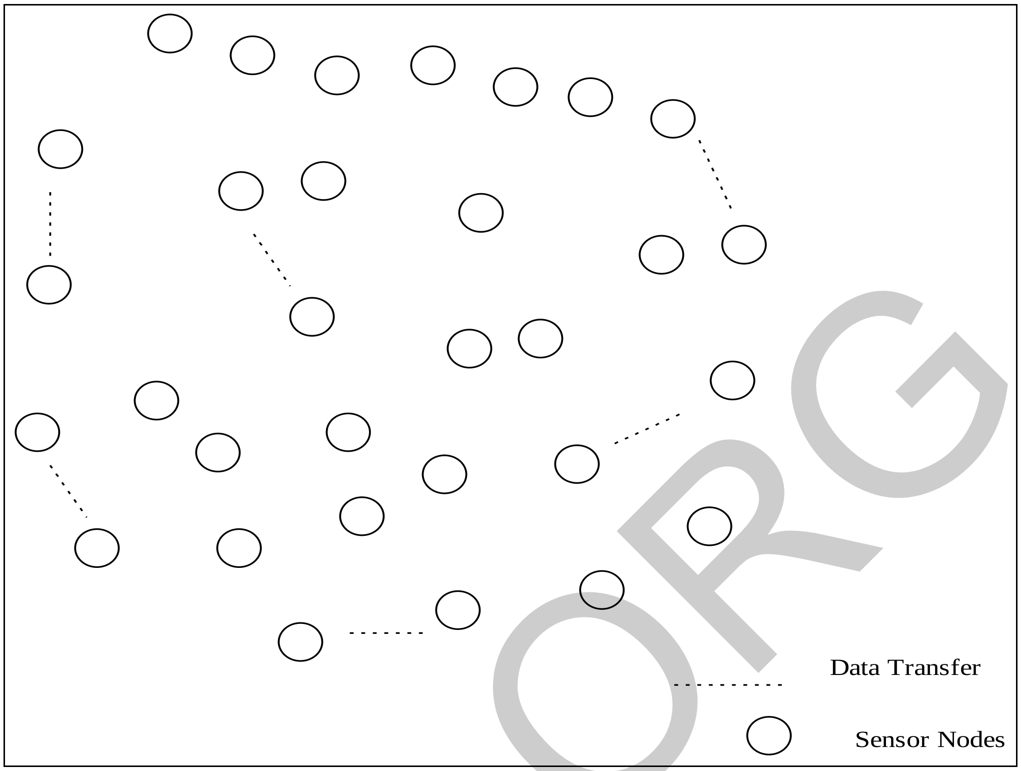

Fig.1. Network Region

(a) Sybil Attack

In a Sybil attack, a malicious node pretends theidentity of several nodes, by doing so undermining the effectivenessof fault-tolerance schemes, such as the redundancy ofmany routing protocols. Sybil attacks also pose a significantthreat to geographic routing protocols. Location aware routingoften requires nodes to exchange coordinate information withtheir neighbors to efficiently route geographically addressedpackets. By using the Sybil attack, an adversary can act inmore than one place at the same time [5].

(b) Security Problems

Securityproblem may happen at network layer and include: data integrity attacks, byaccessing, modifying, or injecting traffic; denial-of-service attacks; flow-disruptionattacks, by delaying, dropping, or corrupting data passing through, but leaving routingtraffic unmodified; passive eavesdropping; resource depletion attacks, by sending datawith the objective of congesting a network or draining batteries; signaling attacks, byinjecting 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 datapacket 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 maliciousdevice adopting multiple identities illegitimately and theadditional identities are known as Sybil nodes. The Sybil attack can occur in a WSN since itoperates without a central authority which can verify theidentities of each communicating entity [9]. Becauseeach entity is only aware of others through messagesover a communication channel, a Sybil attacker maytake different identities during transmission of messageto the legitimate node. To defend against Sybil attack itis 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.

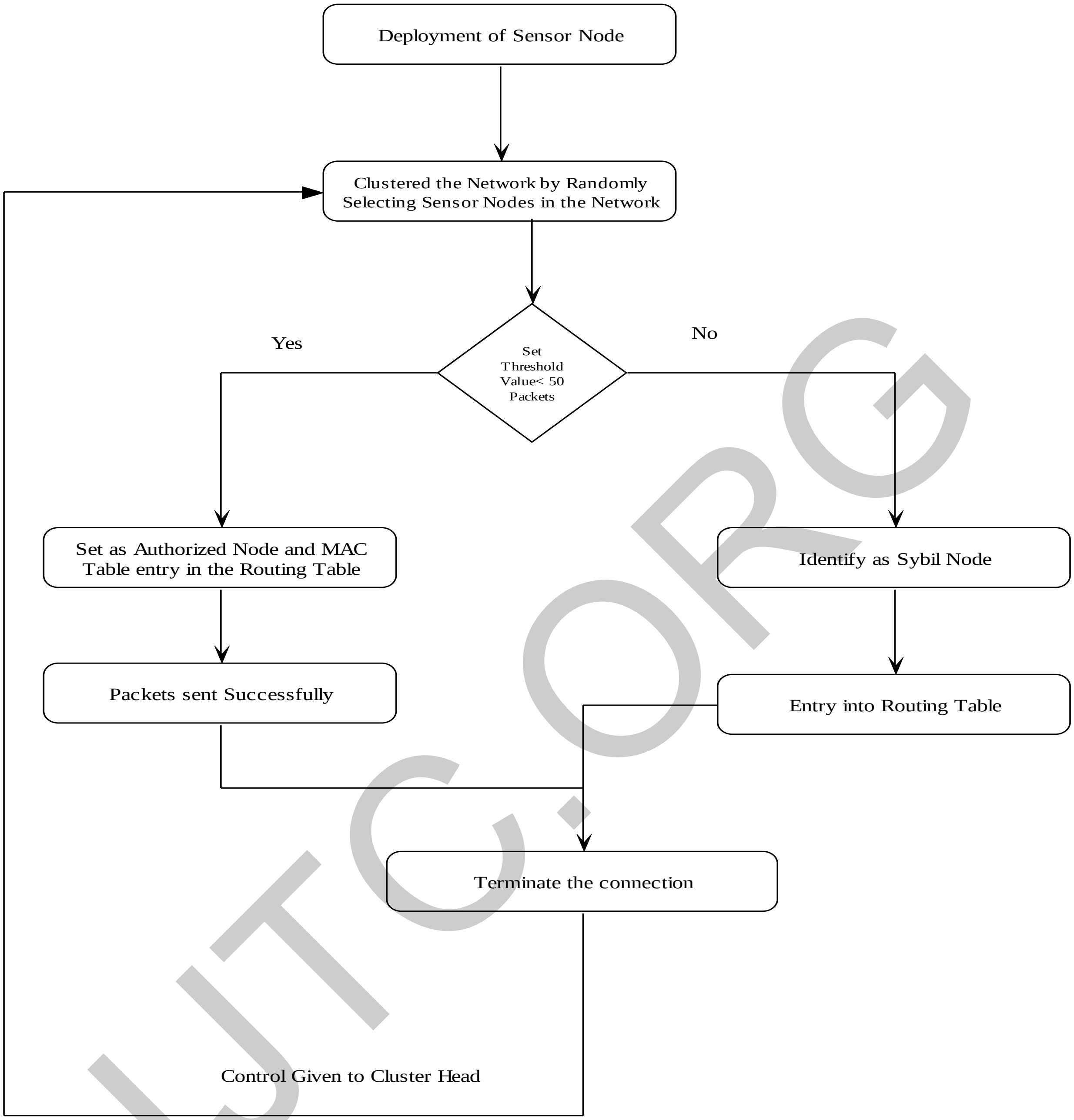
Deployment of Sensor Node
Clustered the Network by Randomly Selecting Sensor Nodes in the Network
Yes
No
Set Threshold Value< 50 Packets
Set as Authorized Node and MAC Table entry in the Routing Table
Identify as Sybil Node
Packets sent Successfully
Entry into Routing Table
Terminate the connection
Control Given to Cluster Head

Fig.2. Flow Chart of Proposed Work

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

[1] Xuhui Chen, "Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes", 978-1-4244-6495-1, pp. 2863 – 2867, IEEE, 2010.

[2] Vinod Kone., "QUORUM- Quality of Service in Wireless Mesh Networks", Springer Science Business Media, LLC, 2008.

[3] Yong-Sik Choi, "A study on sensor nodes attestation protocol in a Wireless Sensor Network", 978-1-4244-5427-3, pp. 1738-9445, IEEE, 2010.

[4] Yuling Lei, "The Research of Coverage Problems in Wireless Sensor Network", 978-0-7695-3901-0, pp. 31 – 34, IEEE, 2009.

[5] Yan Zhang,JijunLuo,Honglin Hu,"Wireless Mesh Networking Architectures, Protocols and Standards",Auerbach Publications,2007.

[6] T.P.Lambrou and C.G. Panayiotou, "A Survey on Routing Techniques Supporting Mobility in Sensor Networks" In Proceedings of the 5th international conference on Mobile Ad Hoc and Sensor Networks (MSN'09). pp. 78-85.

[7] Y. Han and Z. Lin. 2012. A geographically opportunistic routing protocol used in mobile wireless sensor networks. In proceedings of the 9th IEEE international conference on Networking, Sensing and Control (ICNSC). pp. 216-221

[8] Mark A. Perillo, Wendi B. Heinzelman, "Wireless Sensor Network Protocols",Taylor & Francis Group, LLC, 2006,pp.36-813.

[9]Himika Sharma, Roopali Garg, "Enhanced Lightweight Sybil Attack DetectionTechnique",IEEE, 2014,pp.476-481.

[10] KuanZhang,XiaohuiLiang,Rongxing Lu and Xuemin Shen, "Sybil Attacks and Their Defenses in the Internet of Things",IEEE,2014,pp.372-383.

[11] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks", Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[12]M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[13]N. H. Mistry, D. C. Jinwala and M. A. Zaveri,"MOSAODV: Solution to Secure AODV against Black hole Attack", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009.pp.42-45.

[14] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", In Proceedings of the 36th Hawaii International Conference on System Sciences,2003, pp. 57-61.

[15]O. Younis, S. Fahmy, Heed, "A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks", IEEE Transactionson Mobile Computing 3 (4) (2004) 660–669.

[16]Poongothai T. and Jayarajan K., "A non-cooperative game approach for intrusion detection in Mobile Adhoc networks", International Conference of Computing,Communication and Networking (ICCC), 18-20 Dec 2008, , pp 1-4.