Optimized Secure Routing Mechanism to prevent Sybil Attack for WSN

Priti Rani[1], Er.Baljeet Kaur[2]

[1]Research Scholar, Sri Sukhmani College of Engg & Technology, Derabassi

[2]Assistant Professor, Department of ECE, Sri Sukhmani College of Engg & Technology, Derabassi,

***Abstract*— Wireless sensor network is recently act as most vulnerable to the attacks such as Sybil attack. In recent time, there are many network suffered by Sybil attack due to easy authenticity to the Sybil attack creating nodes. In this paper we have proposed a centralized sink based elimination of the Sybil attack with help of better key management system which assign secret keys at the start of the network to every node and later, these keys is used to detect un even behaviour in network. Mechanism used basic functionality of RSSI (Receive Signal Strength Indicator) along with cluster heads in wireless sensor network to provide easy working of secret keys for detection of the attack. Keys are used to provide unique identity to the cluster head selected which is regenerated by base station after particular interval of time. In this paper, we analyse the behaviour of Sybil attack and provide solution for detection and elimination of Sybil attack which provide better results in term of throughput and Packet delivery ratio than the previous research. Network Simulator is used for experimentation with wireless sensor node under Sybil attack.**

***Keywords*— Sybil Attack, Security Mechanism, RSSI, Route Management, Wireless Sensor Network.**

I. INTRODUCTION

Last decade bring good communication features in wireless sensor network. Due to growth of new protocols in wireless sensor network, energy efficiency increase significantly and communication is going with rapid acceptance from many user end applications. Sensor networks represent a significant improvement over traditional sensors but also got vulnerable to attacks while providing more efficiency in term of energy saving. The process of routing protocol is to provide refined path for routing in between sensor node from sensor field to sink node, and further used to send useful data. When most routing protocol is designed, the security trouble never been taken into consideration fully. Hence any research which provides good efficiency and better security mechanism is worth to study. On demand routing protocols are one of the type of protocols which are in existence from long time and provides good level of energy saving while communication but it is also a truth that these are most vulnerable to many attacks easily. Protocols such as leach, used alternatively to on demand protocols and provide similar behaviour. We present problem of these protocols when network is suffered by Sybil attack and provided the mechanism based on reactive protocols which provide better communication as compared to the leach protocol. The proposed mechanism start detection with basic RSSI value from cluster heads and proceeded further with key matching process.

II. ATTACKS IN WIRELESS SENSOR NETWORKS

Wireless sensor networks are more vulnerable to security attacks than traditional wired networks, due to the open communication and unreliable medium of communication. Network operates in different layers and layers operates according to the fixed rules defined by network parameters so it is due to this fact, network communication is vulnerable to attackers. Especially in case of wireless sensor network, in which sensor nodes are remotely controlled and can't be accessed physically every time; attacks are easy to launch. Attacks on sensor net-works can be classified into attacks on its layers like physical, link, network, transportation, and application layers. Attacks can also be classified based on the capability of the attacker, such as sensor level and laptop-level. A powerful laptop-level adversary can do much more harm to a network than a malicious sensor node, since it has much better power supply, as well as larger computation and communication capabilities than a sensor node.

III. SYBIL ATTACK

Sybil attack is known as the scenario where wireless nodes take unauthorized identity from other nodes. Usually wireless sensor network defined as a malicious device illegitimately taking on multiple identities.

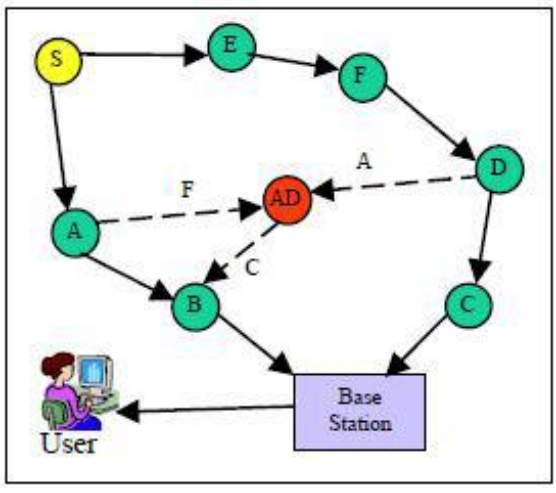

Figure 1: Sybil Attack [4]

In Sybil attack [4], an adversary can appear to be in multiple places at the same time. In other words, a single node presents

multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of legitimate nodes. Figure 1 demonstrates Sybil attack where an adversary node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and 'A' as to 'D' so when 'A' wants to communicate with 'F' it sends the message to 'AD'.

IV. Proposed Work

In this paper, we have provided solution for limitations of network by proposing a secure routing scheme for reactive protocol for preventing the Sybil attack. In proposed work, sink maintained a pair wise distribution list of keys which provides unique identity to the cluster head selected which regenerated by base station after particular interval of time. Receive Signal Strength Identifier is used for judging the distance.

The idea of introducing multiple keys can be viewed as the combination of the basic key pool scheme and the above RSSI approach. The base station randomly generates a pool of n key spaces each of which has unique private information. Each sensor node is assigned k out of the m key spaces. If two neighboring nodes have one or more key spaces in common, they can compute their secret key. If the key matches, then nodes is considered as Sybil node and is eliminated by sending message to sink and sink to all other nodes.

V. Objectives

To achieve desired results for proposed work, following are the objectives for fulfilling the requirement of the work.

- To achieve better solution for Sybil attack in wireless sensor network by introduction of the unique mechanism which will avoid Sybil attack with avoidance of unique key replication?
- To provide solution for Secure and stable mechanism for detection and avoidance of Sybil attacks in wireless sensor network by introducing prevention mechanism.
- To find the performance under Sybil attack in wireless sensor networks by comparing it with simple wireless sensor network.

VI. Methodology

Our experimentation is focused on the eliminating the Sybil attacks from the wireless sensor network. Network Simulator is used for experimentation. We have started with deployment of sensors in the field and unique keys are assigned to the sensors.

The simulation randomly generates 100 points in the range of 1000 m × 1000 m plane. Various energy values are provided to nodes and base station. Magnify Coefficient value based on distance is assigned to simulation.

Cluster heads are selected on bases of residual energy of the nodes. Nodes with higher residual energy are selected as the candidate for cluster head selection. Receive signal strength identifier is used to fetch cluster head and cluster information.

Now in wireless sensor network, there is a threshold value for the number of cluster heads in the whole network. Threshold value is calculated after selecting cluster heads in the network.

If two neighboring nodes have one or more key spaces in common, they can compute their secret key. If the key matches, then nodes is considered as Sybil node and will be eliminated by sending message to sink and sink to all other nodes. This mechanism will prevent the Sybil attack and will also useful in detection of the attack.

VII. Result and Discussions

The Basic parameters used for experimentation are shown in table 1. We use Network Simulator 2 for simulation with generates 100 points in range of 1000 m × 1000 m plane.

Parameters	Value
Simulator	OPNET
Simulation Time	900
No of nodes	100
Energy Consumption	60 nJ/bit
Basic Energy	5 J
Pause Time	100 sec
Speed	11 mps

Table 1: Parameters used for experimentation

Results obtained for the detection of Sybil attack is compared with previous research [1] in which the similar approach have been followed. We have applied previous work's scenario in term of throughput and packet delivery ratio. The proposed work provides better results on different nodes of the network as compared to previous research [1] done.

COMPARISON OF PROPOSED AND PREVIOUS WORK IN TERM OF PACKET DELIVERY RATIO

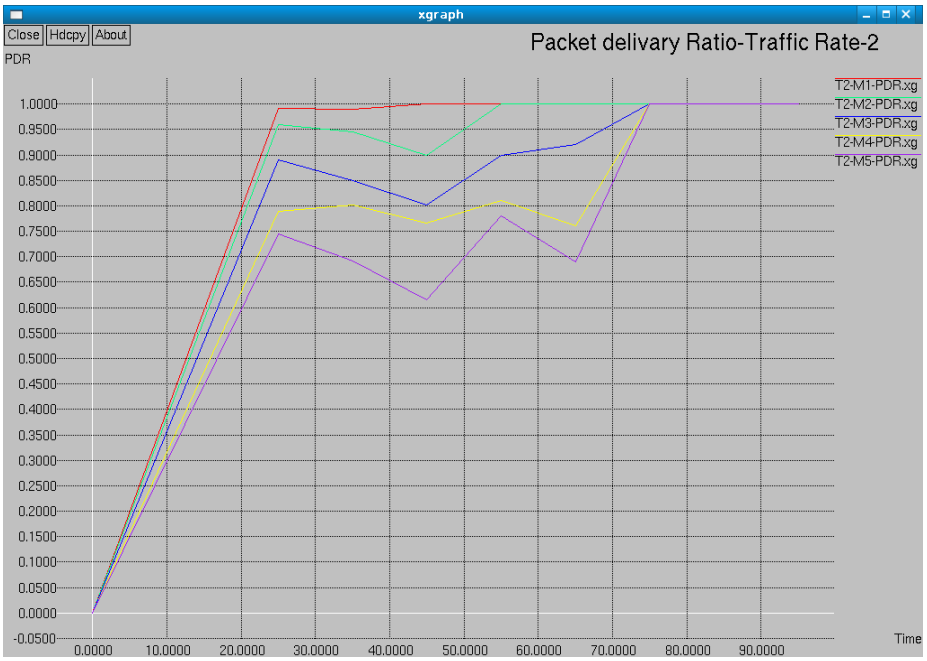

Figure 2: Packet Delivery Ratio comparison of proposed and previous work

The performance of network is compared in above figure (Figure 5) and it show that the red line representing the proposed work in term of packet delivery ratio.
Blue line shows the previous work with different PDR values on different nodes of the wireless sensor network communication.

COMPARISON OF PROPOSED AND PREVIOUS WORK IN TERM OF THROUGHPUT

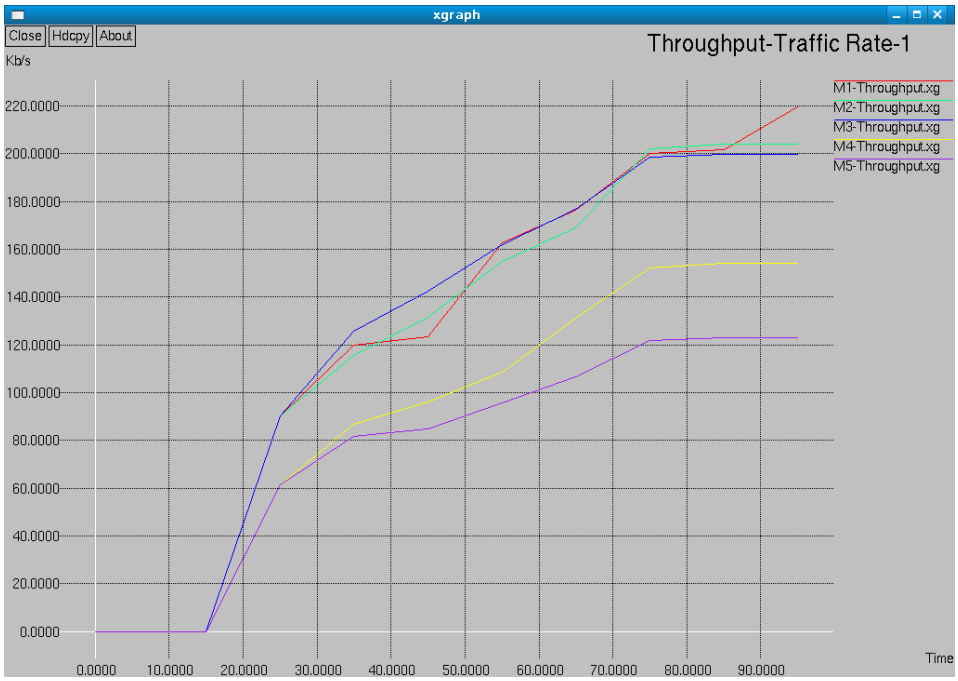

Figure 3: Throughput comparison of proposed and previous work

The performance of network is compared in above figure (Figure 3) and it show that the red line representing the proposed work in term of throughput.
Blue line shows the previous work with different throughput values on different nodes of the wireless sensor network communication.

VIII. CONCLUSIONS

In this paper, performance of the wireless sensor network communication has been analysed. Cluster heads are selected on bases of residual energy of the nodes. Nodes with higher residual energy are selected as the candidate for cluster head selection. Receive signal strength identifier is used to fetch cluster head and cluster information.
Attacker nodes have been applied in experimentation and properties of Sybil attack has been considered for finding the effects of attacks on network. Further for elimination of the Sybil attack, a new concept based on secret key with collaboration of RSSI values have been proposed and implemented. Proposed mechanism successfully detects and eliminates the Sybil attack with fast detection of Sybil attacker nodes. The proposed results shows better throughput and packet delivery ratio values than previous work consider for experimentation.

REFERENCES

[1] Shanshan Chen, Geng Yang, Shengshou Chen," A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks", 2010 International Conference on Communications and Mobile Computing, vol 2, issue 4, pp 33-39, 2010.

[2] Shio Kumar Singh, M P Singh, and D K Singh," A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology, vol 1, issue 2, pp 9-17, May to June 2011.

[3] Preeti Sharma," A Review of Attacks on Wireless Sensor Networks", Journal of Information Systems and Communication, vol 3, issue 1, pp.-251-255, 2012.

[4] J.R. Douceur, "The Sybil Attack", in 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), vol 3, issue 3, pp. 251-260, March 2002, LNCS 2429, 2002.

[5] Karen Hsu, Man-Kit Leung, Brian Su, "Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks", IACSIT International Journal of Engineering and Technology, Vol.2, No.4, pp 1793-8236, August 2010.

[6] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig," The Sybil Attack in Sensor Networks: Analysis & Defenses", Center for Computer and Communications Security at Carnegie Mellon under grant DAAD19-02-1-0389, April 26–27, 2004.

[7] Nitish Balachandran, Sugata Sanyal, "A Review of Techniques to Mitigate Sybil Attacks", Int. J. Advanced Networking and Applications, vol 4, issue 1 pp 1514-1518, 2012.

[8] Amol Vasudeva1 and Manu Sood, "Sybil Attack on Lowest Id Clustering Algorithm in the Mobile Ad Hoc Network", International Journal of Network Security & Its Applications (IJNSA), vol.4, no.5, pp 17-23, September 2012.

[9] S.Sharmila, G Umamaheswari," Detection of Sybil Attack in Mobile Wireless Sensor Networks", [IJESAT] International Journal of Engineering Science & Advanced Technology, vol 2, issue 2, pp 256 – 262, 2012.