Detection and Prevention of Sinkhole Attack in Wireless Sensor Network using Armstrong 16-digit Key Identity and GAN Network

Dhivya M[1], Shanthana Roja A P[2], Sneha K V[2], Selva Lakshmi S[2]

[1]*Assistant Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India.*

[2]*Student, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India.*

Corresponding Author: shanthanaroja99@gmail.com

Abstract: - Wireless Sensor Networks (WSNs) have collection of sensor nodes to collect information about the surrounding environment. WSN are used in many areas especially in health applications, industrial monitoring, military applications, environment monitoring applications etc. The sensor nodes have limited battery power and less memory and they are deployed in dangerous environments where they are not physically protected so they are subjected to different types of security attacks. One of the most common attacks is sinkhole attack where intruder capture or insert nodes in the sensor field that advertise routes to the base station. In this paper, a phenomenon is proposed against sinkhole attacks which detect malicious nodes which generate duplicate keys and cause power loss and packet drop. We are using AODV routing protocol to ensure secured transmission of data. Further, the system uses an ARMSTRONG 16-digit key to detect the malicious nodes which are trying to connect in the communication channel. GAN network is applied to dump the false nodes by identifying the fake ID data. Simulation results show that the proposed method successfully detects the sinkhole nodes for large sensor fields.

Key Words: — ***Wireless Sensor Network, Sinkhole attack, AODV, Armstrong 16-digit key identity, GAN network.***

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of nodes with sensors to collect the information about the surrounding environment of a specific area. Wireless Sensor Network measures environmental conditions like sound, temperature, wind, humidity, pollutants, motion, vibration, pressure and so on. The user communicates with the network via sink or base station. The sensor nodes communicate among themselves using radio signals. The sensor nodes deployed in the network gather information about the surrounding environment and it performs specific instructions or provide sensing samples according to the queries sent from the control site. The nodes have limited storage capacity, communication bandwidth and processing speed.

WSN has many applications. It includes health applications such as tracking the location of patients and overall monitoring of patients, industrial monitoring such as machine health monitoring, data logging, and wastewater monitoring and structural health monitoring which includes monitoring the changes to the material and geometric properties of engineering structures like buildings, flyovers, bridges, roads etc., military applications such as enemy tracking and security detections, environment monitoring applications such as agricultural monitoring, habitat monitoring, indoor living monitoring, green house monitoring uses these networks. In the field of transport systems WSN is used for monitoring of traffic, dynamic routing management, and monitoring of parking lots etc. The sensor nodes from sensor networks are dropped to the field of interest and are remotely controlled by a user. Sensor nodes are insecure and frequently deployed in dangerous environments which causes security attacks like sinkhole attacks, Sybil attacks, jamming or packet injection attacks, wormhole attacks etc.

Sinkhole attack is a type of attack, which hack a node within the network or launches a malicious node in the network to attract the network traffic by advertising its fake routing update. It causes packet drop, energy loss, increases delay and reduces network performance and delivery ratio. Sinkhole attack causes some other attacks like acknowledge spoofing attack, selective forwarding attack, drop or alter routing information.

Manuscript revised March 28, 2021; accepted March 29, 2021. Date of publication March 31, 2021.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898

II. LITERATURE SURVEY

Kenneth E. Nwankwo et al proposed a framework which comprises two stages. The first stage involves problem formulation and planning, dataset description with design. In the next stage Enhanced Ant Colony optimization detection is implemented on NS-3.29 simulator, flowchart and pseudocode. This algorithm improves sinkhole detection rate and reduces false alarm in wireless sensor networks.

Karthigadevi et al proposed a decentralized sinkhole detection mechanism using neighbor discovery, neighbor density estimation technique. Every node in the network performs neighbor discovery and by using the neighbor details, neighbor density is estimated. The sinkhole is identified based on the traffic pattern of all neighbors. This method reduces the overhead of collecting snapshots and routes.

Zhaohui Zhang et al proposed a model in which RMHDS algorithm is used. The base station catches the information of all neighbor nodes according to the location of all nodes in the network then hop database is established. M nodes are randomly selected and M minimum hop routes to the sink are established. If the number of passed nodes is greater than threshold it is determined as the malicious node and if the hop difference between the node and its neighbor is greater than the threshold then that node is determined as the malicious node. This model increases the detection rate and reduces the false positive rate.

Abdulmalik Danmallam Bello et al proposed Delphi technique to overcome sinkhole attack. The malicious node is detected by calculating the delay per hop for each node existing in the path, the malicious node is removed from the network and a new path is formed from the source to the destination to send the data packets. This technique reduces packet loss, delay and increases the throughput.

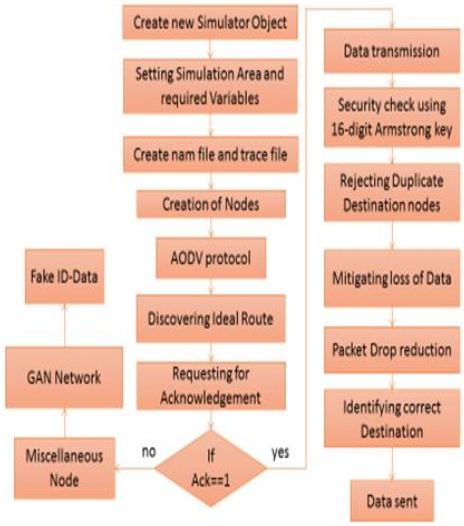
Mohammad Wazid et al proposed a scheme in which hierarchical wireless sensor networking is divided into various disjoint clusters. The anomaly detection and the type of sinkhole are identified using sinkhole node existence and identification algorithm. Then CH blacklists those malicious nodes and sends alarm to its cluster members. The detection algorithm used here requires a lesser number of message exchange which results in low communication cost.

III. EXISTING SYSTEM

Threshold Sensitive Energy Efficient Sensor Network (TEEN) is used as the routing protocol. Homomorphic encryption is used to detect and prevent sinkhole attack. For simulation Omnet++ is used with static nodes. TEEN is not much efficient if periodic reports are needed. Homomorphic encryption increases the overhead and energy consumption is high.

IV. PROPOSED SYSTEM

In the proposed method, Adhoc On-Demand Distance Vector (AODV) routing protocol is used. The malicious node is detected using Armstrong 16-digit key identity. Further, GAN network is used to dump the malicious node.



A. Simulation Environment

The proposed method is implemented in NS2. Topology, number of nodes and properties such as type of channel, interface queue, antenna, routing protocol and simulation time are set. NAM file, trace file and nodes are created.

B. Routing Protocol

The source and destination nodes are defined and the route from source to destination is selected using AODV routing protocol which supports both unicast and multicast. To find the valid route from source to destination RREQ is forwarded after receiving the request if the intermediate node has a valid route to destination then it prepares a route reply message else it will forward the request to other nodes. During communication the malicious node steals the identity of the base station and the sensor nodes send data to the malicious node instead of the base station. Key distribution is performed by the base station to all the sensor nodes. Data is sent to the

base station from sensor nodes only after verifying the key of the base station. The base station calculates the key with Armstrong number.

Table.1. Simulation Parameters

Simulation Parameters	Values
Area of Simulation	1000*1000 meters
Channel Type	Wireless
Number of nodes	40
Type of Routing protocol	AODV
Internet protocol type	TCP
Link Layer	LL
Queue Type	Priority Queue
Antenna Model	Omnidirectional
Max Packet	50
Transmission speed	1.2 Mbps
Bandwidth	20 MHz

C. Detection of sinkhole attack

The 16-bit Armstrong number is generated from various colour combinations and it is very difficult to crack. Using the concept of Armstrong number, the keys which are distributed in the network are generated. The final key is formed by concatenating the unique identification of each node with the key. The original base station provides its identification when the sensor node asks for it but the malicious node cannot provide its identification, it is detected as the malicious node.

D. Isolation of malicious node

Generative Adversarial Network (GAN) is applied after the detection of the malicious node. This network helps in identifying the fake ID and the fake ID data is stored in order to dump those false nodes for effective data transmission.

V. RESULTS AND DISCUSSION

The proposed method is implemented in NS2. Using the above discussed method our network is protected from sinkhole attack and the throughput time is increased, packet drop and delay are reduced.

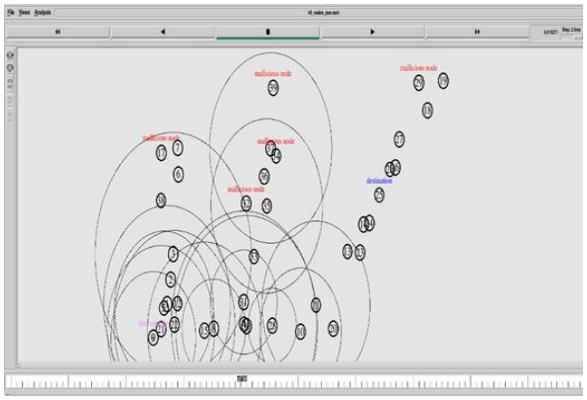


Fig.1. Data sharing in WSN

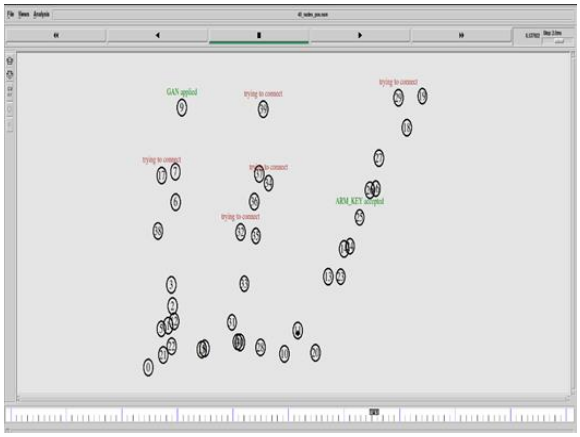


Fig.2. Prevention of Sinkhole attack

VI. CONCLUSION AND FUTURE WORK

In the proposed method we have presented a new technique to detect and prevent sinkhole attacks in wireless sensor networks. The AODV routing protocol used is scalable to a large number of terminals. The use of Armstrong number and GAN network mitigate the sinkhole attack. The proposed method does not require additional hardware. No extra communication is used for the purpose of detecting and isolating sinkhole attacks. Proposed technique is also applicable when sinkhole nodes advertise high quality link, strong transmitted power etc.

In future we can use some other techniques to further reduce the energy consumption and also, we focus on analyzing and studying sinkhole attack in the context of other routing protocols.

REFERENCES

[1]. Martins, D., Guyennet, H.: Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. 2010 13th International Conference on Network-Based Information Systems. pp. 313–320. IEEE (2010).

[2]. Chen, C., Song, M., Hsieh, G.: Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. 2010 IEEE International Conference on Wireless Communications, Networking and Information Security. pp. 711–716. IEEE (2010).

[3]. Rong, C., Eggen, S., Cheng, H.: A novel intrusion detection algorithm for wireless sensor networks. 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE). pp. 1–7. IEEE (2011).

[4]. M. T. Kurniawan and S. Yazid, "Mitigation strategy of sinkhole attack in Wireless Sensor Network," 2017 International Workshop on Big Data and Information Security (IWBIS), Jakarta, Indonesia, 2017, pp. 119-125.

[5]. K. E. Nwankwo and S. M. Abdulhamid, "Sinkhole Attack Detection in A Wireless Sensor Networks using Enhanced Ant Colony Optimization to Improve Detection Rate," 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (Nigeria Comput Conf), Zaria, Nigeria, 2019, pp. 1-6.

[6]. K. Karthigadevi, S. Balamurali and M. Venkatesulu, "Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to Detect and Prevent the Sinkhole Attack in Wireless Sensor Network," 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Tamilnadu, India, 2019, pp. 1-4.

[7]. Zhang, Z., Liu, S., Bai, Y. et al. M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks. Cluster Comput 22, 7677–7685 (2019).

[8]. Abdulmalik Danmallam Bello, Dr. O. S. Lamba, 2020, How to Detect and Mitigate Sinkhole Attack in Wireless Sensor Network (WSN), International Journal Of Engineering Research & Technology (IJERT) Volume 09, Issue 05 (May 2020).

[9]. Wazid, Mohammad & Das, Ashok Kumar & Kumari, Saru & Khan, Khurram. (2016). Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Security and Communication Networks. 9. 10.1002/sec.1652.