SECURING DSR PROTOCOL DEFENDING AGAINST SYBIL ATTACK IN MANET

Mrs. D.M. Vijayalakshmi[1], Sharadh R[2], Vignesh.K[3] ,Subash.A.L[4]

[1]Assistant Professor, Department Of Computer Science Engineering, Adhiyamaan College Of Engineering (Autonomous), Hosur, Tamil Nadu, India.
[2,3,4]Student, Department Of Computer Science Engineering, Adhiyamaan College Of Engineering (Autonomous), Hosur, Tamil Nadu, India.

Abstract

Mobile ad hoc networks (MANETs) are infrastructure-free networks in which nodes are free to move in any direction. These networks use specific routing protocols that can create a path between nodes that are not within transmission range of each other. Because MANETs are easy to configure, they are mostly used in areas where infrastructure is not available, such as military and rescue operations, etc. Due to the open approach, MANETs are always vulnerable to external and internal attacks such as Denial of Service (DoS), Flooding, Worms hole, Black hole, Gray hole Sinkholes etc. There is no central point of administration. In this project, we focus on the Sybil attack. An SYBIL attack is an individual type of association layer attack in a specially selected mobile network. In this attack, a fake hub is introduced that has a direct path to reach the target. So it collects the entire packet from the source and drops it. Nowadays, it is very difficult to secure the network against such attacks. The Dynamic Source Routing (DSR) algorithm uses caching concepts to store all newly created routing paths in mobile ad hoc networks. Route caching aggressively uses DSR. With source routing, it is possible to cache each overhead path without causing loops. Forwarding nodes cache the source path from a packet and forward it for future use. The destination also meets all the requirements. Thus, the source learns many alternative paths to the destination, which are stored in the cache. Here, we propose a novel approach to prevent Sybil attacks in DSR based on route caching. In this approach, once a Sybil node is detected in the MANET during path construction, we pass the Sybil node id to the DSR path function. In this function, routes are ready to be added to the route cache; however, adding each route to the route cache is decided by parsing those routes for the presence of a Sybil node id. This process uses only the normal time of the caching process. In this project, we propose a cache-based Sybil attack prevention algorithm for DSR routing protocols in MANET. Simulations in NS-2 show that our proposed mechanism greatly reduces the packet drop rate with a very low false positive rate.

Keywords: Mobile Ad Hoc networks (MANETs), Sybil Attack, Denial Of Service (DOS), Dynamic Source Routing (DSR), Route Caching, Packet Drop Rate, NS-2.

I. INTRODUCTION

Wireless sensor networks (WSNs) are emerging technology consisting of small, low-power devices that integrate limited computing, sensing, and radio communication capabilities. The main goals of wireless sensor network deployment are remote monitoring and information gathering. WSNs are typically used in open, uncontrolled environments, often in hostile territories. But the open nature of wireless communication channels, lack of infrastructure, rapid deployment procedures, and hostile environments where sensor nodes are deployed make them vulnerable to a wide variety of security attacks. Especially in emergency response operations, such as after a natural disaster such as a flood, tornado, or earthquake, a wireless sensor network can be used for real-time feedback. Thus, emergency rescue will rely on this particular type of network. WSNs can be disabled by interfering with packet transmission within the network through sinkhole attacks, Sybil attacks, jamming or packet injection attacks, and wormhole attacks. Our project mainly focuses on sinkhole attacks and proposes a technique to isolate these attacks in WSNs.

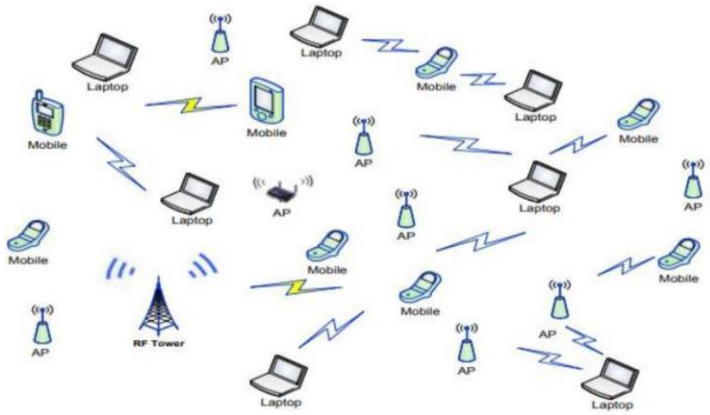
OBJECTIVE

Increase performance by comparing throughput, end-to-end delay and packet drop ratio.

- Monitor the performance of the proposed algorithm, DSR.
- Detects and prevents Sybil attacks in MANETs using a cache-based black hole attack prevention approach.
- Perform the mitigation process simultaneously with the delay without increasing the time delay value.
- Maintain the same performance even as the number of nodes and network size grows.

WIRELESS SENSOR NETWORK

Wireless sensor networks (WSNs) are a new class of wireless networks that are becoming very popular in a large number of civilian and military applications. A WSN consists of a set of interconnected small sensor nodes that communicate with each other and exchange information and data. These nodes acquire information about the environment, such as temperature, pressure, humidity or pollutants, and send this information to the base station. It sends information to the cable network or activates an alarm or action depending on the type and size of the monitored data.



The performance of a wireless network mainly depends on the type of end-to-end. We will present a simulation scenario focused on enabling network security through network throughput, and packet transmission between nodes within the scenario using cryptographic algorithms; in our simulator, we use the RC5 algorithm to encrypt packet information that is transmitted between nodes.

The simulation principles and strategies adopting the separated object model and using the two languages C++ and tclNS2 fulfill the achievement of simulation for specific protocols and configuration nodes and the creation of a network simulation environment. The parameters that are used in the scenario use supported software such as NAM to perform further study and simulation processes and analyze the results. First, we set the topology and configuration of node properties, as well as MAC layer properties such as address type, protocol type, channel type, simulation time, modulation type, tx, rx, idle, sleep power and wireless transmission method. Below are the parameters of the simulation scenario and the layout of the nodes before the information is transferred between them. The following is the propagation of all nodes and the coverage of nodes at a certain time. Then there is information transfer (package information) between nodes and coverage the radios are single and send information (secure information), and this information is converted from plain text to ciphertext (Kurdistan Regional Government) between node (0) and node (24).) as a scenario. Furthermore, at a certain time, information is transferred between two scenarios (node0 and node 24, node 17 and node 9), also information is transferred between nodes (17 and 9). Packages will drop after the simulation is complete.

II. LITERATURE REVIEW

A network should flexibly respond to changing conditions through a routing protocol, otherwise, all routing criteria must be predetermined and remain unchanged. Proactive, reactive, and hybrid routing protocols are three types of routing protocols defined based on path discovery. Proactive routing protocols are widely known as table-driven protocols because they exchange their routing information among all sensor nodes in the network. Reactive protocols are classified as tableless routing protocols because they create paths only when required and hence the time consumed to find the path is relatively more. A hybrid routing protocol also includes reactive and proactive protocol capabilities to provide better routing results. [1] Recommended EEPR (Energy-Efficient Probabilistic Routing) algorithm to control packet forwarding of routing requests, which would improve network lifetime and improve in reducing packet loss. Simulations are used to verify that the EEPR and AODV algorithms have a longer network lifetime and use the residual energy of each node, thus slightly improving the routing setup latency and the routing probability is continuously reduced. [2]A offers details on swarm intelligence for IoT routing protocols commonly used for MANETs and wireless sensor networks (WSNs). MANET and WSN have almost the same routing mechanism. The Swarm mechanism is considered to achieve maximum optimization and reliability to meet wireless network requirements. [3] IDS can be categorized based on their detection method as misuse and anomaly. Based on the response, IDS can be divided into active and passive, and from the decision point of view into cooperative and autonomous. The authors report three IDS-related works on the LEACH protocol. First, a watchdog-based

IDS is designed to catch the attack on each phase of rule applications, and second, a specification-based IDS is designed. The third method, namely CUSUM IDS, is proposed based on path construction, which uses information about the normal path and the malicious path for intrusion detection. [4] In this work, the authors propose a security mechanism based on TESLA (Timed Efficient Stream Loss-Tolerant Authentication) to protect the LEACH protocol. The BS acts as a key distribution center (KDC) and periodically transmits the TESLA key to the sensor nodes. The nodes send the data along with the node formation membership certificate to the CH. Until then, the CH aggregates and transmits the sensed data to the BS. [5]

III. EXISTING SYSTEM

The main objective of this existing system is to provide a benchmarking analysis of the performance of routing protocols using the ViSim tool that integrates the Ns2 simulator.

- This tool focuses on MANET (Mobile Ad-Hoc Network) protocols for proactive - DSDV (Destination-Sequenced Distance-Vector Routing) DSR and AODV (Ad-hoc On-demand Distance Vector).
- Throughput, Good Location (packet and packet size) and Routing Load (packet and packet size) are parameters to compare between routing protocols for performance analysis.
- This tool can be modified in the future to better analyze different routing protocols.

IV. DISADVANTAGES

- Due to security checks during the routing mechanism, the delay has been increased by 0.2 to 0.5 seconds.
- The quality of service of the mitigation technique used in this existing method to improve network performance is quite low compared to other techniques.

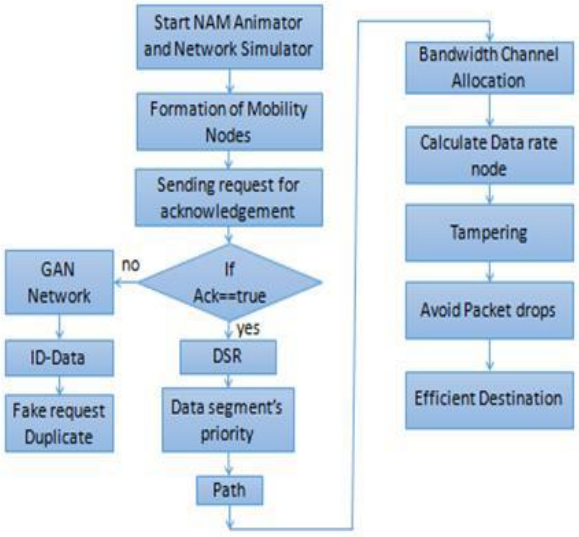
V. PROPOSED SYSTEM

- In this proposed technique, we present a new approach to prevent Sybil attacks in DSR using DSR's route cache mechanism.
- When detecting a Sybil node or a misbehaving node, during path construction processing, we need to get the Sybil node ID and pass it to add to the DSR path function.
- Functional paths are ready to be added to the route cache, but before adding each path to the route cache, we parse those paths for the presence of the Sybil node id.
- If a Sybil node appears in a path, we simply need to list that path and add all the remaining paths for the intended source-destination pairwise communication.

VI. ADVANTAGES

- This process uses only the normal time of the caching process.
- This minimizes latency compared to previous Sybil attack detection mechanisms.
- Packet drop rate is drastically reduced.

VII. ARCHITECTURE DESIGN



VIII. MODULE

There are five modules in this system:

- Initialization of NAM animator and Network
- Simulator Module
- Acknowledgement Request Module
- DSR Module
- Dumping Black node Module
- Destination Module

Modules description

1. Initialization of NAM and NS2 Module:
In this module, a Network simulator (NS2) is started for simulation purposes and Network Animator (NAM) for displaying the simulated network. The required circuit nodes will also be created.

2. Acknowledgement request Module:
This module sends a confirmation request to the target node. If the request is accepted, the next process will continue, otherwise, the request will be sent again. If a fake confirmation is received, the ID will be copied as a fake ID.

3. DSR Module:
In this module, the Dynamic Source Routing (DSR) algorithm is used to create an ideal path for the transfer of data. It stores all the newly constructed routes by using the route caching concept.

4. Dumping Black node Module:
In this module, the path containing the black hole will be dumped and the remaining stored routes will be considered for the transfer of data from source to destination.

5. Destination Module:
In this module, the desired data will be transmitted from source to destination by selecting the efficient route path for transmission with a high data transmission rate and reduced loss of data.

IX. SYSTEM FUNCTION

1. NS2

NS2 stands for Network Simulator Version 2. It is an open-source event-driven simulator designed specifically for research in computer communication networks.

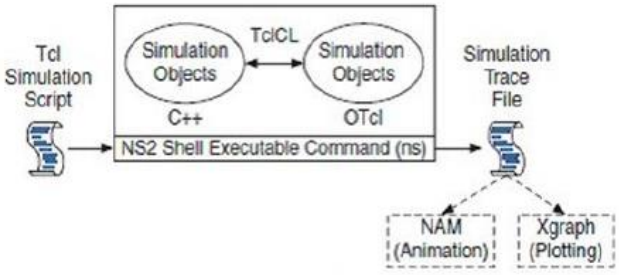
Features of NS2

1. It is a discrete event simulator for networking research.
2. It provides substantial support to simulate a bunch of protocols like TCP, FTP, UDP, HTTP and DSR.
3. It simulates wired and wireless networks.
4. It is primarily Unix based.
5. Uses TCL as its scripting language.
6. Otcl: Object-oriented support
7. Tclcl: C++ and OTcl linkage
8. Discrete event scheduler

Basic Architecture

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up the simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and the OTcl are linked together using TclCL

.



Basic architecture of NS.

2. LINUX (Ubuntu)

Overview

Ubuntu is by far the most popular Linux distribution for running web servers from the sites they analyze, "used by 47.3% of all sites that use Linux", and Ubuntu alone powers more sites than Microsoft Windows, which powers 28.2% of all sites. , or 39% of the share held by Unix (which includes Linux and therefore Ubuntu). All Linux/Unix distributions have a combined performance of more than twice the number of hosts than Windows for websites based on W3Techs numbers. Ubuntu and Debian alone (on which

Ubuntu is based, with the same package manager and therefore managed in the same way) account for 65% of all Linux distributions for web services; Ubuntu usage surpassed Debian (for such server usage) in May 2016.Ubuntu is the most popular Linux distribution among the top 1000 sites, gaining about 500 of the top 10 million sites daily.

Features of Ubuntu

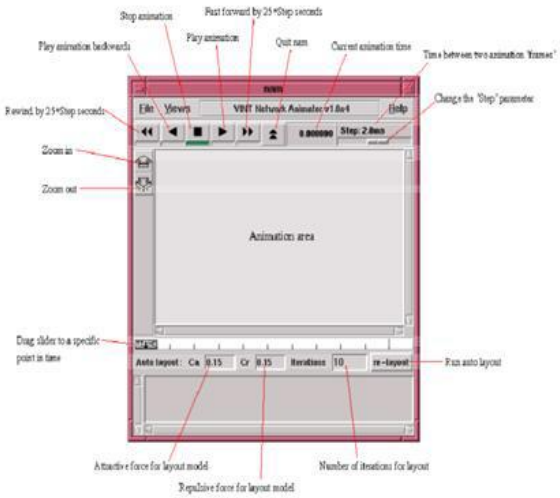
The default installation of Ubuntu includes a wide variety of software that includes Libre Office, Firefox, Thunderbird, Transmission and a few light games such as Sudoku and Chess.

- Many other software packages are accessible from Ubuntu's built-in software (formerly Ubuntu Software Center) as well as from other APT-based package management tools.
- Many other software packages that are no longer installed by default, such as Evolution, GIMP, Pidgin, and Synaptic, are still available in the repositories and can be installed using the main tool or any other APT-based package management tool.
- There are also snap and flatpack packages for various distributions, both of which allow software such as Microsoft software to be installed on most major Linux operating systems (such as any currently supported version of Ubuntu and Fedora).

2. NETWORK ANIMATOR [NAM]

NAM is a Tcl/TK-based animation tool for displaying network simulation routes and real-world packet routes. It has a graphical interface that can provide information such as the number of dropped packets on each link. The network animator "NAM" which is located in the initial position and starts moving the node wirelessly started in 1990 as a simple tool to animate packet trace data. Nam started at LBL. NAM was developed in collaboration with the VINT project. It is currently developed as an open-source project hosted on Source forge.

- This trace data is usually derived as output from a network simulator such as ns or from actual network measurements such as using tcpdump.
- We can run NAM either with a command
- 'name'
- where " is the name of the NAM trace file that was generated by NS or can be run directly from a Tcl simulation script to visualize node motion.
- The NAM window is shown in the following figure
- We can use NAM in a network simulation by creating a name trace file and then running the name trace file on a TCL script.



3. MANET in NS2

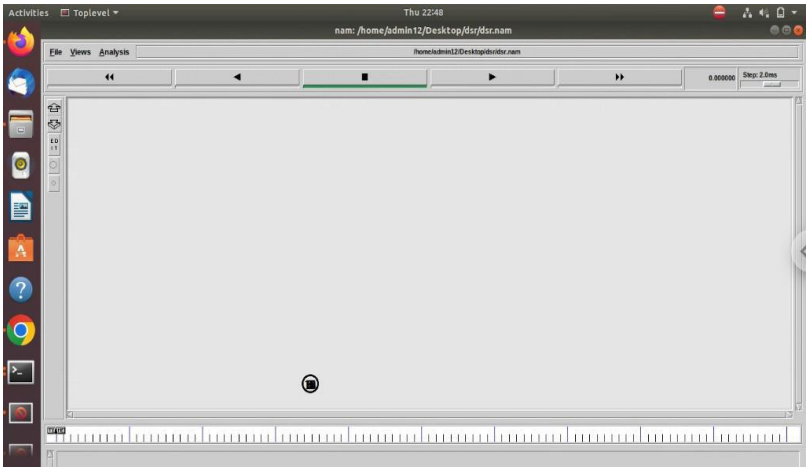
Unlike infrastructure-based wireless networks, a mobile ad hoc network, or MANET, does not depend on fixed infrastructure for its network traffic. A MANET is an autonomous and short-lived association of a group of mobile nodes that communicate with each other via wireless links. A node can communicate directly with nodes that lie within its communication range. If a node wants to communicate with a node that is not directly in its communication range, it uses intermediate nodes as routers. From a simulation perspective, the primary component in designing a mobile advertising network is the mobility model, while other components include node configuration, random topology, and communication model. In the mobility model, the mobility of a node from one location to another can be enabled using the "saddest" keyword in the Tool Command Language (TCL) script. The specifications for the node's target location include the x, and y coordinates along with the velocity. Nodes are configured with the components of the channel, network interface, radio propagation model, medium access control (MAC), ado routing protocol, interface queue, link layer, topographic object, and antenna type. In a dynamic topology, the neighbours of each node vary according to the location of that particular node. Nodes in the ado network communicate using a communication model.

.

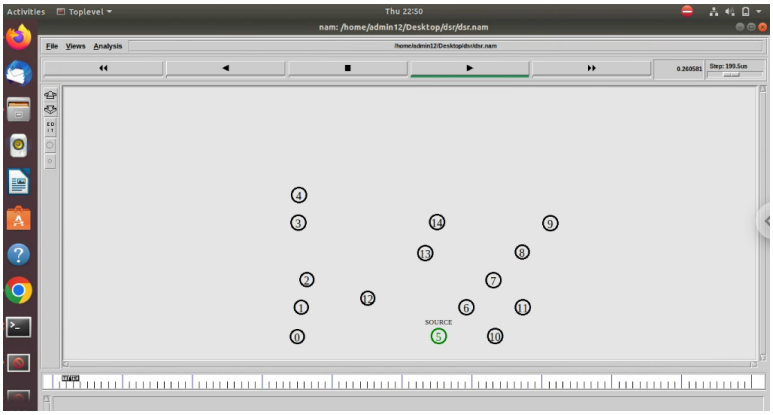
X. RESULTS AND DISCUSSION

The secure transmission date from source to destination is completed without any interruption and reduces packet drop and time delay.

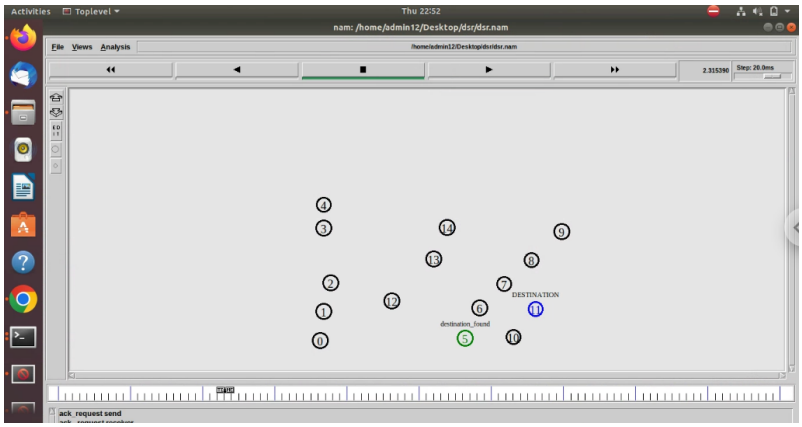
The number of nodes is present in the Nam animator which is located in the initial position and starts moving the node wirelessly.



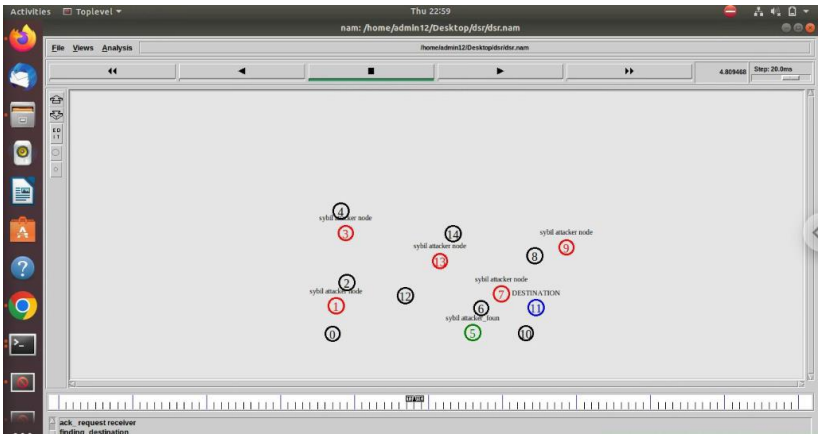
The nodes are moving randomly and assign node names to check the source node is presented in the TCL code, the node number assigns 5th node and sends that request to the destination.



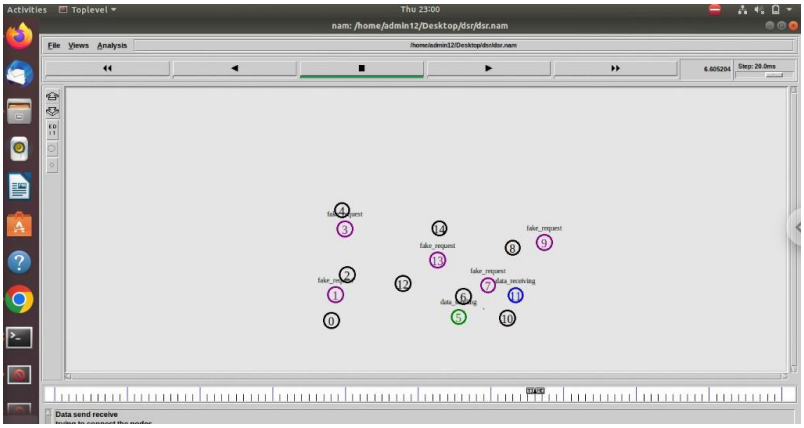
Here the source node sends ack request to a destination which will conform to the destination and in predefined in code are user-defined nodes.



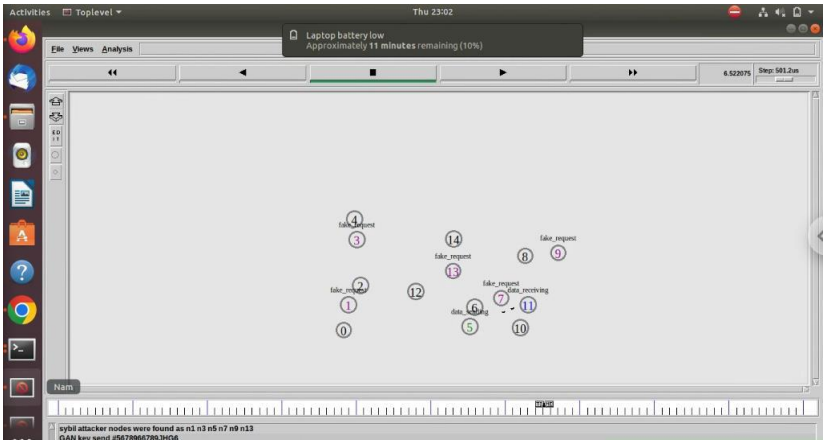
The nodes are random and the source sends the data to the destination. Here some Sybil attacker nodes are formed to avoid the data transmission from source to destination in MANET (Mobile -Ad hoc network).



The fake nodes are sending data to the source which acts as a destination node here the source node sends some GAW key which contains 16 digital passkeys which are used to conform to the destination without any interruption.



Finally, the nodes conform to the destination and transmit the data without only time delay and also reduced packet drop while transferring the data.



XI. CONCLUSION

In this Project, we have presented a new technique to detect black hole attacks in wireless sensor networks. Our proposed system implements the DSR protocol as a routing protocol. It does not require additional hardware, node location or sending any information to the base station. No extra communication is used to detect and isolate black hole attacks. DSR protocol is a more efficient routing protocol generally as it uses cache memory to save all the possible routes that can be enhanced for communication purposes. Further, the use of a GAN network is applied to mitigate security by identifying the fake ID data of the miscellaneous nodes. Proposed techniques are also applicable when black hole nodes advertise the high-quality link, strong transmitted power etc. In such cases also, our system manages to detect and isolate such attacks in wireless sensor networks.

REFERENCES

[1] *A. Mouiz, A. Badri, Evaluating the Power Consumption of Routing Protocols for Wireless Sensor Networks under Different Metric Parameters, IEEE paper 2020.*
[2] *S.H. Park, S. Cho, and J.R. Lee, Energy-Efficient Probabilistic Routing Algorithm for Internet of Things. In 2019 4th International Conference on Recent Trend on Electronics, Information, Communication & Technology, IEEE.*
[3] *S. S. Roy, D. Puthal, S. Sharma. Building a Sustainable Internet of Things: Energy Efficient Routing Using Low-Power Sensors Will Meet the Need, IEEE 2021.*
[4] *S. Gupta and V. Grover, "Survey of intrusion detection techniques in LEACH", 2019.*
[5] *S. Ramachandran and V. Shanmugam, "An approach to secure leach using tesla-based certificate", 2021.*
[6] *Martins, D., Guyen net, H.: Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. 2010 13th International Conference on Network-Based Information Systems. pp. 313–320. IEEE (2020).*
[7] *Pandey, A., Tripathi, R.C. A Survey on Wireless Sensor Networks Security. Int. J. Comput. Appl. IJCA. 3, 43–49 (2019).*
[8] *Ngai, E.C.H., Liu, J., Lyu, M.R.: An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Comput. Commun. 30, 2353–2364 (2021).*
[9] *Tumrongwittayapak, C., Varakulsiripunth, R.: Detecting Sinkhole attacks in wireless sensor networks. ICROS-SICE International Joint Conference. pp. 1966–1971 (2019).*
[10] *Tumrongwittayapak, C., Varakulsiripunth, R.: Detecting sinkhole attack and selective forwarding attack in wireless sensor networks. 2009 7th International Conference on Information, Communications and Signal Processing (ICICS). pp. 1–5. IEEE (2020).*
[11] *Coppolino, L., D'Antonio, S., Romano, L., Spagnuolo, G.: An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies. 2010 5th International Conference on Critical Infrastructure (CRIS). pp. 1–8. IEEE (2019).*
[12] *Krontiris, I., Dimitriou, T., Giannetsos, T., Mpasoukos, M.: Intrusion detection of sinkhole attacks in wireless sensor networks. In: Kutyłowski, M., Cichoń, J., and Kubiak, P. (eds.) ALGOSENSORS'07 Proceedings of the 3rd international conference on Algorithmic aspects of wireless sensor networks. pp. 150–161. Springer-Verlag, Wroclaw, Poland (2020).*