Sixth Int. Conf. on Computer Systems, Data Communication and Security, CDCS

An IoT Provisioning against Cyber Malware

Syed Abid Husain[1] and Dr. Baswaraj Gadgay[2]
[1]Asst.Prof , Dept E&C, BLDEA's College of Engg & Tech, Vijayapur 586103
Email: abidsyed4u@gmail.com
[2]Professor & Regional Director, VTU RO, Kalaburagi 585105
Email: baswaraj_gadgay@vtu.ac.in

***Abstract*—The significant challenges faced in todays wireless network comprising the Internet of Things (IoT), are Security and Privacy. Lack of user's literacy and sturdy protocols used has resulted in security weakness associated with the routing protocol like AODV. In our study we saw that malicious objects have a prudent effect on cyber defense mechanism. A peer node while communicating faces a malicious node,waiting to seduce this communication. Once the Malicious node gets identified, the source nodes ensures that its routing path in the next attempt should avoid the malicious node path. Simulation results demonstrates that our method minimizes delay and enhances through-put while identifying and avoiding malicious node.**

***Index Terms*— Internet of Things,AODV, Privacy Interoperability,Automation,Packet loss rate(PLR).**

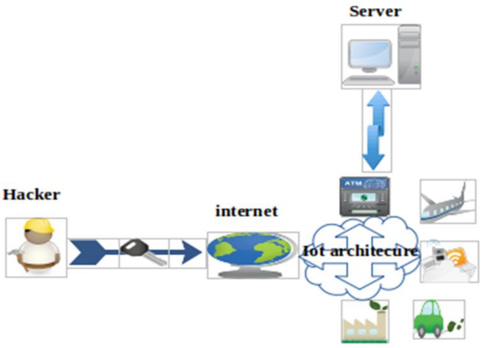
I. INTRODUCTION

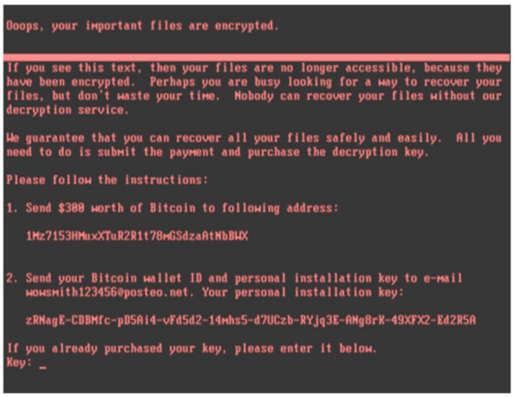
The latest trends and updates, informs us of the exponentially growing IoT population that is connecting to the web worldwide. But at the same time, Cybersecurity risk and malicious application access to confidential data have also increased. This is attributed to ignorantly using the system key and lack of system renovation. Cracking the database is mainly due to weak security measures adopted. The network security expert sees IoT as the sensitive towards Cyber intrusion. It's due to weak security protocols and policies. Different types of malware have been developed by hackers to infect IoT devices. Hackers sends deceitful emails,pretending to be from reputable companies to induce individuals to reveal personal information[6].High profile attacks are continuously increasing in the corporate world. Even a system using MQTT (Message Queuing Telemetry Transport) protocol which is designed to handle uneasy situation in network application like IoT,may come under attack e.g Dos[20].Therefore the need of the hour is to develop a competent security mechanism to face such Cyber threats.

The application of IoT involves several areas such as resourceful home, smart supply chain customization environment and intelligent monitoring [1][2], therefore the importance of network security is obvious. The integration of real objects into any wireless network harbors several Cybersecurity threats for businesses. An attacker can compromise the entire system by shutting it down using, Denial of Service (DoS), Man-in-the-Middle (MITM) and others techniques, against critical IoT infrastructures. To master these challenges, IDS plays an essential role as an important tool in the IoT security framework for information systems and conventional networks. Therefore, to improve the security of IoT, it is imperative to build a high-performance IoT intrusion detection system element [3]. The speed of 5G mobile truly connects all things and urban life. But at the same time loss of information & equipment related to the Internet of Things increases exponentially. Therefore it's

Grenze ID: 02.CDCS.2023.6.510_1

crucial to augment the performance of the Internet object intrusion detection system [5](Figure 1).
The rest of the paper is organized as follows. Section II describes security vulnerabilities and related work. Section III describes the routing protocol used. Section IV describes System Model, that works to mitigate routing attacks.





```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

Figure1:Intrusion attempt

II. Security Vulnerabilities and Related Work

Security vulnerabilities are considered a major concern in wsn Therefore it's the most researched area. The various types of attacks like DoS,WH SH etc,possess a major threat to network security. Few such attacks and their countermeasures are shown in TableI. Accessibility from unknown and un trusted Internet sources is common, which increases the risk of hacking. Most of the time, the user is unaware of these developments thus causing unacceptable impairment. Therefore now the awareness has increased. We need to address these few major security issues like Security Privacy Interoperability Automation   to prevent security attacks.

A. Security

IoT has been deployed at a wide range nowadays in contrast to conventional computer networks. Thus making it more exposed to security risk in different ways: Many IoT devices are designed for mass deployment. Sensors are a perfect example. Typically, an IoT installation consists of the same devices that have similar functions. This similarity amplifies any security vulnerabilities that could significantly affect many of them. The application of IoT has resulted in unique challenges that must be addressed. Consumers are expected to trust IoT devices and services are highly protected from attack. especially as this technology continues to become more passive and integrated into our daily lives. The security challenges also increases due to erroneous interconnection of IoT devices This behavior is simply driven by the challenge of the widespread use of uniform IoT devices. The designer of IoT network should ensure that network nodes should not be exposed to any adverse effects. It is vital for a common approach while designing the network[7].

B. Privacy

People's confident should remain intact as negligence can result in iniquity. User privacy and safety in IoT is of vital important. Work in recent past has shown the increased surveillance and monitoring carried out to ensure the same. The reason for privacy concerns stems from ubiquitous integrated intelligence artifacts, where the process of sampling and distributing information in the IoT can be done virtually anywhere. It is due to ubiquitous connectivity of user to the worldwide network,it more easy to gain access to vital personal information[8].

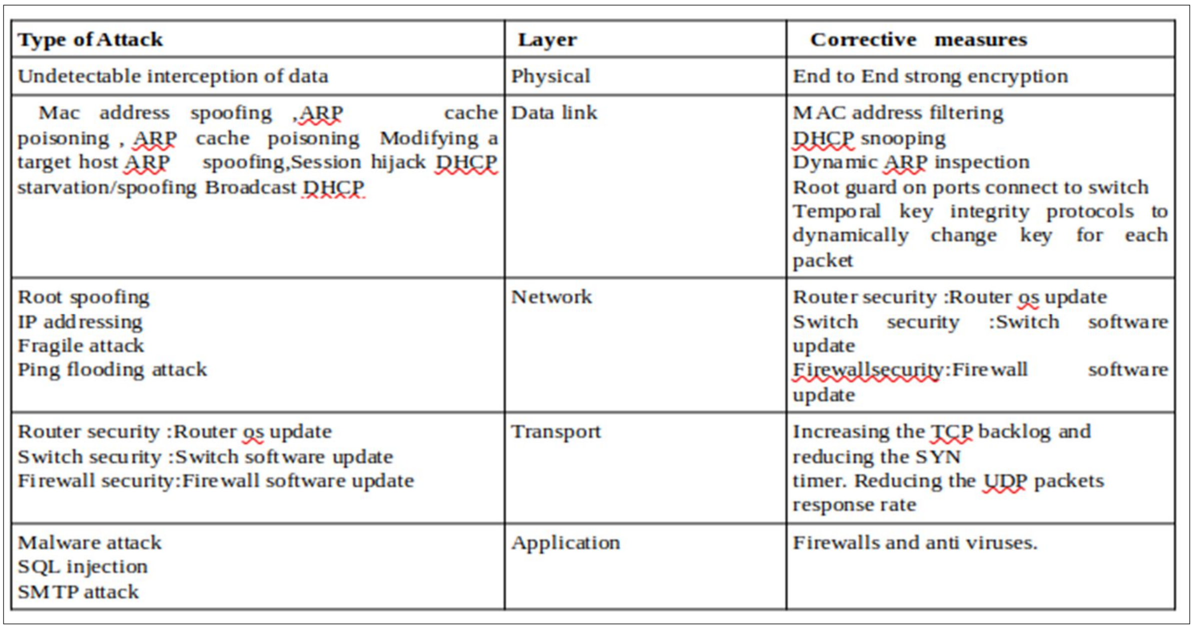
C. Interoperability

Technical implementation can constrain the values of users. Few users may prefer not to buy products and services,whenever they find lack in compliance of IoT devices with respect to their design. Encryption can be put to use to overcome such situation[9]. Security provided at different levels in IoT system can proved to be more effective against perpetrated attacks. This can be accomplished by designing advance   security features.

D. Automation

Network protocols (ex:Wi-Fi, ZigBee)as such ,do not put any restrictions to gain access to an IoT system. A hacker can exploit such automation in IoT to gain access.

TABLE I: ATTACKS AND CORRECTIVE MEASURES



Type of Attack	Layer	Corrective measures
Undetectable interception of data	Physical	End to End strong encryption
Mac address spoofing ,ARP cache poisoning , ARP cache poisoning Modifying a target host ARP spoofing,Session hijack DHCP starvation/spoofing Broadcast DHCP	Data link	MAC address filtering DHCP snooping Dynamic ARP inspection Root guard on ports connect to switch Temporal key integrity protocols to dynamically change key for each packet
Root spoofing IP addressing Fragile attack Ping flooding attack	Network	Router security :Router os update Switch security :Switch software update Firewallsecurity:Firewall software update
Router security :Router os update Switch security :Switch software update Firewall security:Firewall software update	Transport	Increasing the TCP backlog and reducing the SYN timer. Reducing the UDP packets response rate
Malware attack SQL injection SMTP attack	Application	Firewalls and anti viruses.

A round trip delay, round trip path based failure detection is effectively discussed in [19]. Functionality of few routing protocols is at risk. Solution to overcome these problems is suggested in [11-15].eg. In [15] Dokurer et al , recommended few changes in AODV,like avoiding the effort of malicious node to get attach itself on a route to a particular destination. The source node ignores the first two RREP packet then go for the next hop. Black hole node usually reacts to RREP packet more immediately.

III. ROUTING PROTOCOL

A. AODV

To discover a route towards the destination, AODV a proactive routing protocol is used. It takes care of network loop problems, wherein routing packets may circulate indefinitely. The solution to this problem is obtained by removing packets with same sequence numbers. As every node maintains three sequence number counters for three types of packets: a destination counter for RREP, a broadcast counter for RREQ, and a neighbor-probing counter for HELLO.

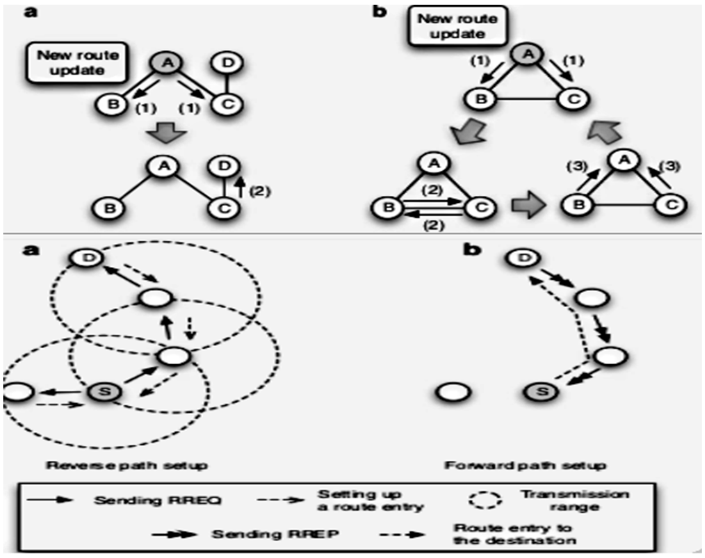
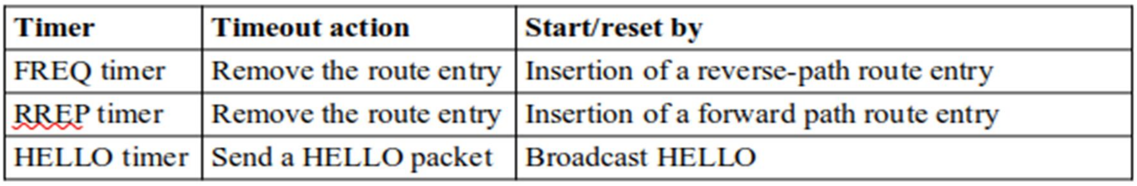


Figure2:A route discovery attempt towards the destination

A node after updating it’s counter by one,marks the packet with the new updated sequence number as shown in figure2a. A new node after receiving this packet checks whether this packet is new one. If it is, then it updates it table,depending upon three different counters,say packet type :RREQ, RREP, or HELLO[10].

TABLE II: ROUTE DISCOVERY



Timer	Timeout action	Start/reset by
FREQ timer	Remove the route entry	Insertion of a reverse-path route entry
RREP timer	Remove the route entry	Insertion of a forward path route entry
HELLO timer	Send a HELLO packet	Broadcast HELLO

B. Route Discovery: Identifying a Route to the Destination

Two important steps are used to discover the route of any destination as shown in Figure2a. Identify the node which owns the routing information. For example:Node “s” in Fig2b,It sends a RREQ to its neighboring nodes. After receiving the query,each node ignores the packet it is already having the same routing information and processes ,if it is a fresh[10]. Any particular node when receives a fresh routing query. It checks if it possesses the desired information. Otherwise it initiates a reverse path setup procedure which records , how to reach to this particular node. The node then increases the no of hop count in the RREQ packet by one and retransmit the RREQ packet. It then sends routing information to the source node in our example, say it’s the node “S”.This is performed by sending a RREP to the source node,which is considered as a path response.

C. Malicious node misguiding the flow

A malicious node say M,seduces into a network and declares that it has the best to a particular destination during a particular routing process as depicted in fig3.This results in route creation that possesses “M”,as one of the routing node. Next time when the source node sends packet to a particular destination,it then passes through a node. The node “M” after intercepting the packets modify it and releases it as per it’s desire as shown in fig3.It is also possible that instead of one, two malicious nodes may cooperate to perform the attack[17],regarding the topology of the network. A source may generate message of any size. But eventually it will be fragmented into fixed or variable size as per demand. An example which shows a peer node communicating with another peer node while a malicious node,waiting to seduce such communication is depicted in Figure 4.

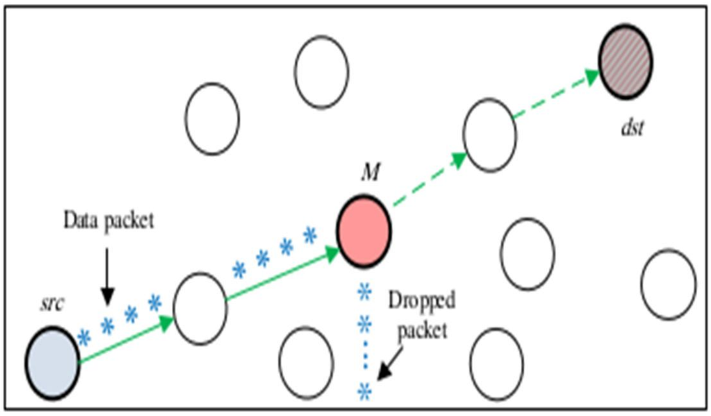


Figure3: Malicious node M seduces the flow

IV. PROPOSED MALICIOUS NODE PATH AVOIDING

A. Attacking Model

We ignore transmission errors, in our work. But transmission errors could be present and the same could be detected and corrected using error detection and correction methods like Block codes. Corrected packets are considered normal arrivals at the destination. The route request creates an entry in many intermediate node's tables. Thus different nodes come to know regarding the topology of network.

In the proposed doctrine, the Malicious node once gets identified, the source nodes ensures that its routing path in the next attempt should avoid the malicious node path. This is illustrated in the flow chart in figure5.

B. Flowchart of the routing process

As illustrated in the flow chart in figure5, the source node (src) initiates the process of route discovery. At every intermediate node the RREQ message is checked,as to whether it is received for first time.if yes,then the node route is sent to the source node otherwise it checks whether,the visited node is the malicious node.If node visited is a malicious node,then information is broadcasted to the entire network.

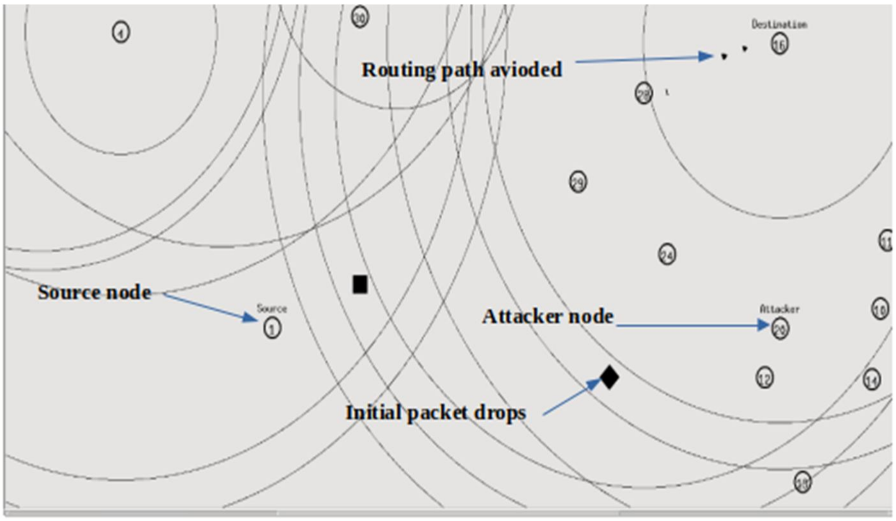


Figure 4:An attacker node mitigation

V. PERFORMANCE EVALUATION

Consider the wireless network as shown in figure4.,The source-destination pairs are spread randomly over the network. The mobility model uses a 'random way point model' in a rectangular field of 600m x 600m with 25 nodes to 100 nodes with a maximum speed of 20 m/s. Other parameters considered are as shown in tableIII. Simulation is performed using ns2.

TABLE III: SIMULATION PARAMETER

Parameter	**Value**
Channel type	Wireless(Two-way propagation)
Area	600x600
Protocol	AODV
Agent used	UDP
Packet Size	512 bits
Rate	600kb
Maxpkts	10000

A. Packet loss rate(PLR)

The no of packet loss that may occurs during any transmission is one of the important performance metric. eg.VoIP.It is defined using the fallowing equation.

$$\text{Packet loss rate} = \frac{\text{Total packet transmitted} - \text{Total packet received}}{\text{Total packet transmitted}} \text{ x } 100$$

The malicious nodes after successful seduction, induces it’s malicious packets in the flow, resulting in packet loss as can be seen in figure6,the peak depict the no of packet loss.

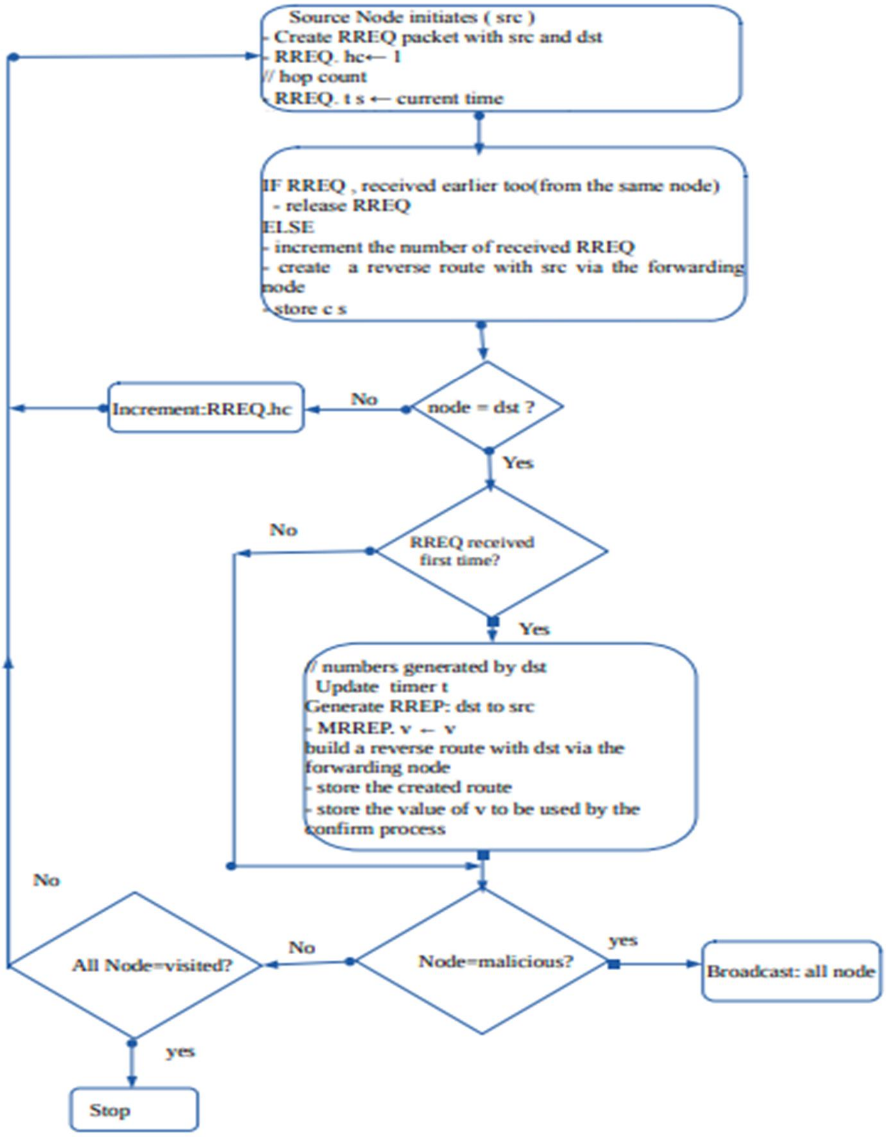

Source Node initiates (src)
- Create RREQ packet with src and dst
- RREQ. hc← 1
// hop count
- RREQ. t s ← current time
IF RREQ , received earlier too(from the same node)
- release RREQ
ELSE
- increment the number of received RREQ
- create a reverse route with src via the forwarding node
- store c s
node = dst ?
No
Increment:RREQ.hc
Yes
RREQ received first time?
No
Yes
// numbers generated by dst
Update timer t
Generate RREP: dst to src
- MRREP. v ← v
build a reverse route with dst via the forwarding node
- store the created route
- store the value of v to be used by the confirm process
No
All Node=visited?
No
Node=malicious?
yes
Broadcast: all node
yes
Stop

Figure 5:Flow chart of the routing process

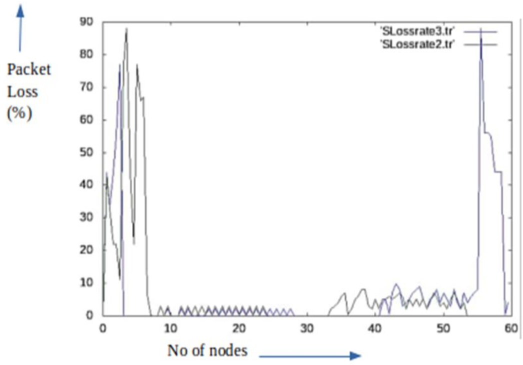


Figure6:No of nodes v/s Packet Loss

B. End to End delay

The time difference that occurs between the first data packet received at destination say t_2 to the time at which the same packet might have been actually sent say $t_{1.}$It is defined using the fallowing equation.

Time delay=Time at which RREQ sent - First data packet received at receiver

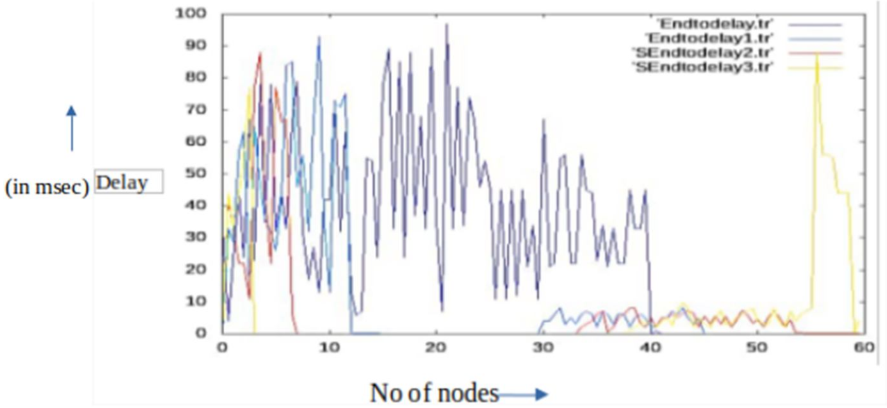


Figure7:End to End delay

Mobility of a node which is sending information,may impact the delay difference that occurs as given in above equation. This is because when the nodes moves ,it results in topological changes as depicted in figure7.

VI. Conclusion

Vulnerability towards a black hole attack as discussed in [18] is effectively dealt with using a diagnostic approach in this work. The work is carried out using ns2.The effective mitigation of malicious node aggression has been discussed. The results shows improvement in delay performance. Our approach significantly treats the malicious node attempt to induce itself as the shortest path node.

References

[1] V. Dastjerdi and R. Buyya, ‘‘Fog computing: Helping the Internet of Things realize its potential,’’ Computer, vol. 49, no. 8, pp. 112–116,Aug. 2016.

[2] J. Li, L. Zhang, X. Feng, K. Jia, and F. Kong, ‘‘Feature extraction and area identification of wireless channel in mobile communication,’’ J. Internet Technol., vol. 20, no. 2, pp. 545–553, 2019.

[3] Z. Jinsheng, ‘‘Design of software architecture stability testing system in IoT framework,’’ Mod. Electron. Technique, vol. 41, no. 20, pp. 118–121,2018.

[4] A. Gupta, R. K. Jha, P. Gandotra, and S. Jain, ‘‘Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network,’’ IEEE Trans. Veh. Technol., vol. 67, no. 1, pp. 618–632, Jan. 2018.

[5] W. Wei, J. Su, H. Song, H. Wang, and X. Fan, ‘‘CDMA-based anti-collision algorithm for EPC global C1 Gen2 systems,’’ Telecommun. Syst., vol. 67,no. 1, pp. 63–71, Jan. 2019.

[6] Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708.

[7] Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28.

[8] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411. [CrossRef]

[9] Zaldivar, D.; Tawalbeh, L.; Muheidat, F. Investigating the Security Threats on Networked Medical Devices.

[10] S. Prakash and A. Swaroop, “A brief survey of blackhole detection and avoidance for ZRP protocol in MANETs,” in Int. Conference on Computing, Communication and Automation (ICCCA), Noida, India, April 2016, pp. 29–30.

[11] Teerawat Issariyakul Ekram Hossain, “Introduction to Network Simulator NS2” Second Edition springer

[12] S. Lu, L. Li, K. Lam, and L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack,” in Int. Conference on Computational Intelligence and Security, Beijing, China, vol. 2, 11–14 Dec. 2009,pp. 421–425.

[13] L. Tamilselvan and V. Sankaranarayanan, “Prevention of co-operative black hole attack in MANET,” Journal of Networks, vol. 3, no. 5, pp. 13–20, 2008.

[14] S. Dokurer, Y. M. Erten, and C. E. Acar, “Performance Analysis of Ad-hoc Networks under Black Hole At-tacks,” in Proc. of the IEEE Southeastcon, Richmond,VA, USA, 2007, pp. 148–153.

[15] A. Yasin and M. Abu Zant, “Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique,” Wireless Communications and Mobile Computing, vol. 2018, Article ID 9812135, 10 pages, 2018

[16] S. Dokurer, Y. M. Erten, and C. E. Acar, “Performance Analysis of Ad-hoc Networks under Black Hole At-tacks,” in Proc. of the IEEE Southeastcon, Richmond,VA, USA, 2007, pp. 148–153.

[17] S. Kalita, B. Sharma, and U. Sharma, “Attacks and Countermeasures in Mobile AD HOC Network – An Analysis,” Int. Journal On Advanced Computer Theory And Engineering, vol. 4, no. 3, pp. 16–21, 2015.

[18] N. Khanna and M. Sachdeva, “A comprehensive tax-onomy of schemes to detect and mitigate blackhole attack and its variants in MANETs,” Computer Science Review, vol. 32, pp. 24–44, 2019.

[19] S. Lu, L. Li, K. Lam, and L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole At-tack,” in Int. Conference on Computational Intelligence and Security, Beijing, China, vol. 2, 11–14 Dec. 2009, pp. 421–425.

[20] Rukhsar begum Shaikh,Abid H Sayed,Z. H. Agusbal“AN ALGORITHM FOR SENSOR NODE FAILURE DETECTION IN WSNs”,International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[21] Mishra, S.; Albarakati, A.; Sharma, S.K. Cyber Threat Intelligence for IoT Using Machine Learning. Processes 2022, 10, 2673. https://doi.org/10.3390/pr10122673.