International Journal of Engineering Sciences &Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Rani, *et al.*, 8(11): November, 2019]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DETECTION AND ISOLATION OF WORMHOLE ATTACK IN MANET

Priyanka Rani*[1] & Harpreet Kaur[2]

*[1&2]Department of Computer Science and Engineering, Lala Lajpat Rai Institute of Engineering and Technology Moga, Punjab, India

DOI: 10.5281/zenodo.3559518

ABSTRACT

The mobile adhoc network is a collection of mobile nodes. These mobile nodes can communicate with each other without using physical infrastructure. MANET has a decentralized network so there is no control on the nodes. Mobile nodes can freely leave or join the network when they want. Sometime malicious nodes can join the network and trigger the wormhole attack. The wormhole attack is the active type of attack which affects network performance to great extent. The wormhole attack is triggered by the malicious nodes. Wormhole nodes do not have any knowledge about the network. They can establish themselves anywhere in the network. Wormholes nodes create tunnel in the network and increase delay in the network. The techniques which are proposed so far are based on the threshold based techniques for the detection of malicious nodes. The threshold value of certain parameters may vary due to various factors like congestion and link failure. When the threshold value of parameters varies then it affects heavily the accuracy of malicious node detection. In the proposed study, a new technique is implemented for the recognition and separation of attacker sensor nodes from the network. The wormhole intrusions are triggered with the help of these attacker nodes in the network. The proposed scheme is utilized in NS2 and it is depicted by the reproduction outcomes that the proposed scheme shows better performance in comparison with existing approaches. The results of proposed two phase verification is compared with CREDND scheme in terms of packet loss, energy, throughput for the detection of malicious nodes and the result shows that the proposed work leads greater performance than the existing one.

KEYWORDS: Wormhole, Delay per hop, attacker, MANETs, Throughput, Delay.

1. INTRODUCTION

In the absence of middle regulator, an arrangement of movable nodes, capable of interacting with various other nodes' packages during the movement in multi-hops is known as MANET. A number of moveable hosts utilizing wireless connections for the purpose of communication with one another are presented inside this network. The nodes can move randomly in any direction because this network has unavailability of any framework and middle regulator. Because of these characteristics, whole nodes presented in this network play the role of a router, where task of package transportation is performed by the source. The safeguarding of routing path is the main area of consideration in MANET [1]. A number of restricted connection mending techniques were projected in the past for the minimization of connection breakdown problems.

An example of this is the interconnection among various machineries approaching from similar region like a company conference for forming an Ad-Hoc network during the availability of network services. After the reception of any information, the movable nodes will send the information further to their neighborhood nodes [2]. The information sent by the intermediary nodes will proceed in the form of a router during the situation while some node requires to forward information to a mobile node but it is beyond the area of sensor node communication. The attainment of immovable routes for transferring information is not achievable because of the random movement of sensor nodes. One of the main problems associated with this network is the unavailability of any steady kind of framework.The sensor nodes presented in this network has the ability of acting like both router and host.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

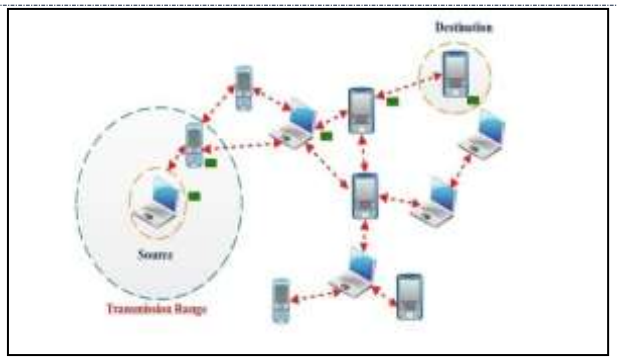

Fig 1: Mobile Ad-hoc Network

The architecture of this network is affected by certain problems like environmental changes, untrustworthy interaction and restricted power of sensor nodes. Because of the restrictions presented in MANET in the form of inadequate bandwidth and sensor node mobility, more attention is required. A number of problems have to be faced during the transferring procedure in MANET like mobile character of sensor nodes presented in the network [3]. The routing procedure failure occurs because of the random allocation of sensor nodes and intermediary sensor nodes' movement in the route. Thus an efficient movability arrangement is needed throughout the direction finding procedure. One other architectural problem associated with MANET is the bandwidth restriction. Hence the implementation of a routing protocol is needed with the help of which problem related with bandwidth constrained can be resolved. This will also prove helpful in the reduction of network cost. Overcrowding and crashing are some other main problems presented in MANET. During the transportation of packages, the instantaneous proceedings of sensor nodes inside the network results in the crashing of information and control packages. The reduction in routing overhead and bandwidth utilization will be ensured by the implementation of routing protocols. The routing protocols will also ensure the on time delivery of packages [4]. Thus a number of routing protocols are required in the network for the implementation of efficient and reliable routing. The intermediary sensor nodes play a very important role in movable and ad hoc network. In these networks, package routing from base station to target relies on the performance of intermediary sensor nodes. For the attainment of efficient, safe and discrete steering of information packages, a number of routing protocols have been invented for MANET. The routing protocols can be categorized in three forms. They are simple protocols, immediate or reactive protocols and integrated or hybrid protocols. A distinct path is created from transmitter to receiver in case of connection breakdown for the continuation of interaction procedure in MANET. The information routing is stopped during the presence of detachment in the path [5]. This results in the reduction of multitasking inside the movable ad hoc MANETs. During the path finding procedure, some strides must be taken like sensor node displacement recognition, connection displacement or non- displacement paths. During the situation of connection breakdown, the data is transferred to the base sensor node. This is done for the minimization of information transferring rate and discovery of some alternating route. With the accumulation of broadcast organizing routing protocol, the problem related to overcrowding is conversed by the crowd commanding approaches. Gathering of information about all the clients is necessary for the continuation and distribution of network reserves. Information about Associative bandwidth and about routers' rows is shared with all other packages which are waiting for their broadcasting turn. The spread out of the row occurs during the presence of large amount of data packages waiting for similar connection. Because of this spread out, packages are plunged. This results in the elimination of demand spread out inside the network [6]. During the constant dropping of packages inside the network, the network is measured as crowded. Because of this overcrowding, the problem of connection breakdown occurs inside the network. an active type of attack named wormhole attack, decreases the performance of network by means of impedance. During the wormhole inclusion, the attacker node obtains the packages and transfers it to some other place through the channel made within the network. In order to influence the performance of network, attacker node directed towards channel after transportation of control packages by base node. The network layer is affected by the wormhole intrusion. The wormhole is called a situation when the system passage is altered through the channel for increasing system delay. The control communications are passed via channel when source sensor node transmit organize message to target for the route development. The responded communications are also passed from channel and the investigation about direct route is performed by the source node [7]. All the packages are altered by attacker sensor nodes via channel or numerous communications after the election of best receiver route by the base.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Because of the attainment of wrong MPRs topology data, the imprecise environmental data is distributed all over the system. After obtaining these fake messages, other sensor nodes can transmit the messages via them for speedy transmission.

2. LITERATURE REVIEW

Sayan Majumder, et.al, (2018) presented a novel arithmetical approach of absolute deviation for the elimination of wormhole intrusion [8]. Because of the implementation of complete divergence clearance and association, the wormhole intrusion can be recognized in the small passage of time. No additional circumstances are needed for the implementation of projected approach. Assumption is made about the presence of less remoteness between base station and target. This means that time consumption for transferring the data packages will be very less. A large amount of time is utilized when the genuine route is trailed. Thus the total time spent during the prevention of wormhole intrusion must be computed carefully. Various experimental outcomes indicated that more precise results are obtained with the help of the proposed approach in comparison with some other approaches. After the measurement of package plunge model, for the identification of wormholes AODV methodology is implemented.

Roshani Verma, et.al, (2017) stated that the main objective of presented study is the recognition and abolition of wormhole intrusion during broadcasting procedures. The presented approached helped in the safety enhancement of ad hoc systems. Thus this network is saved from these kinds of intrusions [9]. Because of the improvement of routing protocols, package transferring rate is augmented and the network cost is minimized. A modification in the table entrance is performed for the identification of high velocity wormhole sensor nodes. For the prevention of integrated and dos intrusions from entering the system, this new technique helped in the implementation of various effective methodologies and thereby ensured the system safety.

Pratik Gite, et.al (2017) presented a novel approach of movable ad-hoc system for using in wireless links. The projected approach is relied on certain parameters like movability, wireless links and self reliance. A novel routing protocol is presented in this study on the basis of which priority levels are assigned to different paths according to their route steadiness [10]. A connection recognition approach is exploited for the design relied on the strength of signal. The projected path idea was executed on AODV protocol. The tested results depicted that the performance of propose approach was superior in comparison with previously used approaches. With the help of proposed approach, problems related to path cost and power utilization has been minimized.
Kavitha T, et.al (2017) stated that main problem of connection breakdown inside movable ad-hoc systems raised because of sensor nodes' movability. A number of methodologies have been already projected for redirecting the packages rapidly. In these approaches, hop count is taken as a constraint but for end to end holdup, accurate outcomes are not given. To overcome this problem, novel routing protocol named instant route migration protocol is projected in this study where route remoteness and hop counts are measured [11]. The experimental results indicated that the highest efficiency and less end to end hold ups are achieved with the help of proposed approach in comparison with certain other approaches.

Sunil Kumar Jangir, et.al, (2016) proposed a comprehensive research work based on wormhole intrusion obtaining in MANET. Some other methods like package leashes, time variant techniques and various other techniques also helped in the recognition and stopping of wormhole intrusions [12]. In association with probable intrusions, various other routing protocols are also studied in this research work. On the basis of their attributes, various wormhole recognition methodologies are evaluated. It is also observed that for the settlement of problems associated with wormhole intrusions different research works are projected. Using different approaches projected in this research work, a robust recognition approach can be acknowledged. Therefore an optimal resolution can be projected for the prevention of wormhole intrusion.

H. Ghayvat, et.al, (2016) presented a safety measure with the help of which recognition and alleviation of wormhole intrusion may be performed [13]. Digital autograph is used for the avoidance of this intrusion. By computing the channeling time utilized by channel, activities of wormhole investigated. For the identification of authentic node from wormhole sensor node, channeling time and threshold values are computed. For the alleviation of wormhole sensor node, digital autograph and muddle sequence approach is utilized. With the use of proposed approach, the efficiency and life span of the network is extended. In comparison with certain other

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

approaches. This results in the reduction of system holdup time. With the help of proposed methodology, quality of service is improved but the abolition of unnecessary faults is still the main concern.

Chitra Gupta, et.al, (2016) stated that a number of techniques for the prevention of wormhole attacks are already available. The proposed approach relied on the alteration of associated approach, gave much precise outcomes. This approach is based on certain factors like package transmitting rate, throughput, directing overhead plunge and so on [14]. For the measurement of unexpected improvement in the system, various other system factors are considered. With the help of presented technique, some other kinds of intrusions are prevented from entering the system. In the near future, this approach can further be improved for the attainment of sensor node movability and vibrant alteration.

3. RESEARCH METHODOLOGY

The wormhole attack is the active type of attack in which delay is increased in the network. When the delay is increased in the network, the latency get increased at steady rate. The proposed methodology is based on the detection of malicious nodes which are responsible to trigger wormhole attack in the network.

The proposed methodology has the two major phases for the detection of malicious nodes from the network.
Phase I : In the first phase, the source node and destination nodes are defined in the network. The source node flood route request packets in the network. The source node calculates the round trip time of the route request and route reply messages in the network. In calculating round trip time, the source start timer when flood route request messages and notice the time for each node when receive route reply packets. The source maintains the list of each node for the route request and reply round trip time. The source selects the best path from source to destination based on the hop count and sequence number. The path which has least hop count and maximum sequence number will be selected as the best path from source to destination. The source node also calculates distance between source and destination based on the number of hops.

Phase II: In the second phase, the malicious nodes get detected from the network. In the second phase, the source node starts transmitting data over the selected path from source to destination. The source calculates the time of data packets at each hop until reach to destination. The time of each hop is compared with the round trip time of route reply packets. The nodes which have significant high time for data packet transmission are marked as the malicious nodes in the network. To isolate malicious nodes from the network, technique of multipath routing is applied in the network. In the multipath routing, when the malicious nodes exits path that path will be ignored in the network.

3.1 Proposed Algorithm

Input : figure of movable sensor nodes
Output : Recognition of attacker node
1. Position system with limited amount of movable sensor nodes
2. Route creating ()
    2.1. Source drive path demand packages in the system
    2.2. The nodes contiguous to target respond with path respond packages.
    2.3. The base choose best route on the base of hop calculation and series figure
3. Compute Threshold rate ()
    3.1. Replicate for the whole sensor nodes
P = Pb *max_p
Until reach to max_p
4. Notice attacker sensor node ()
    4.1. Replicate loop for whole sensor nodes
        If sensor node (i) information rate < P
        Attacker node =node(i)
        Arrival of attacker node
5. Implementation of multipath routing for novel route choosing.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

3.2 Flow chart of Proposed work

Flowchart is a diagram that shows step by step progression through a procedure using connecting lines and symbols. Lines, arrows, rectangle, oval are the symbols of flowchart. Lines and arrows show the sequance of the steps, and the relationship among them.

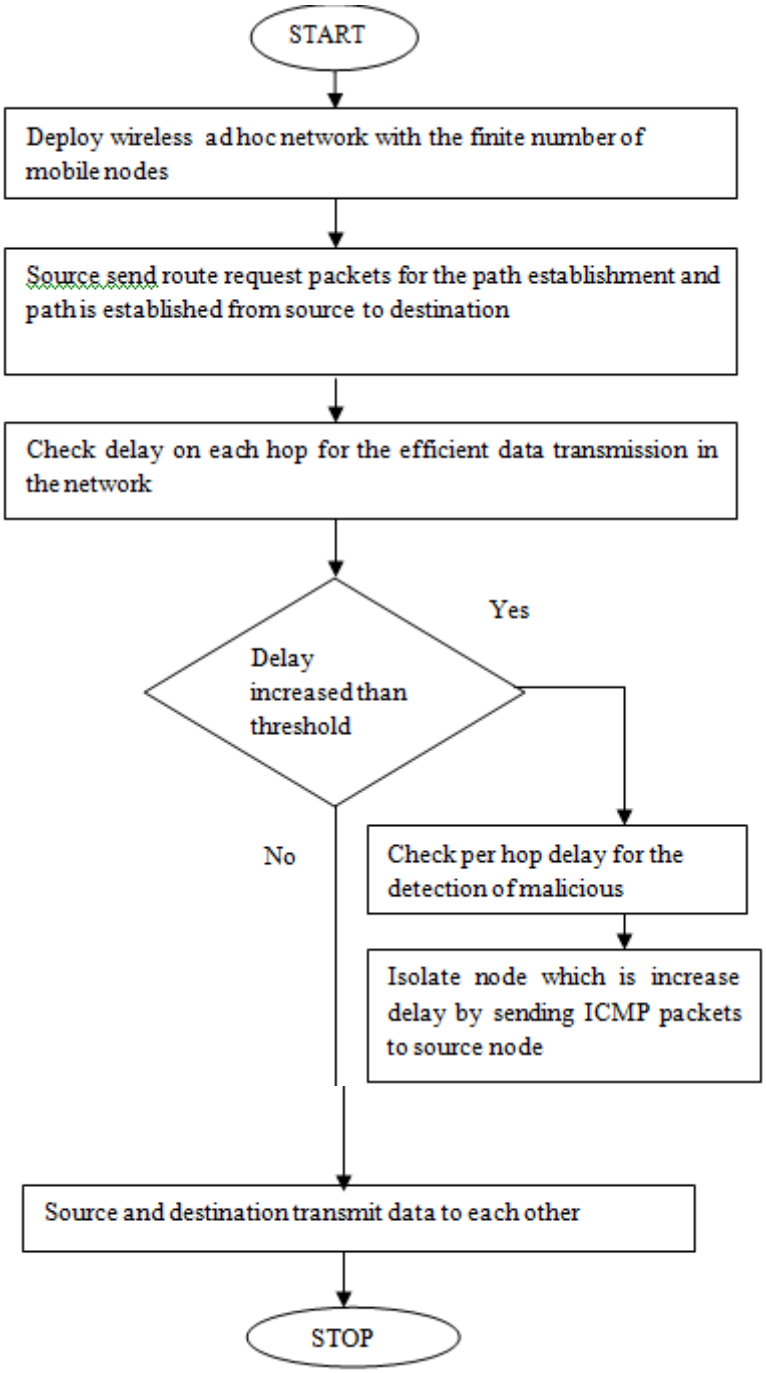

Figure 2: Flowchart of Proposed Work

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

3.3 Objectives

1) To study and analyze the performance of AODV routing protocol in MANET
2) To Trigger wormhole attack in AODV protocol and analyze network performance of MANET
3) To propose an novel techniques to detect and isolate malicious nodes from the network
4) To implement proposed technique and analyze results graphically in terms of energy, throughput and packet loss.

3.4 Performance Metrics

1) **Throughput:** How many packets are effectively transmitted to the target in analyzed by the throughput

   Throughput $= \frac{No\ of\ packets\ Received}{Total\ number\ of\ packet\ send} *$ time

2) **Power :** The power utilization is the parameter which scrutinize the power utilization in the network

   Power Consumption = Number of packets send * per unit power

3) **Packet loss** : The packet loss is the total amount of packets which are misplaced during data broadcasting in the network

   Packet loss= No of packets send - No of packets received

The projected research is carried out in NS2 and the outcomes are investigated by means of various factors.

4. EXPERIMENTAL RESULTS

In this, we study and analyze the perfomance of AODV routing protocol. AODV routing protocol is utilized for the route formation from source to target. The wormhole intrusion is an active kind of intrusion which is launched in the AODV protocol. The performance of AODV protocol is scrutinized under the effect of wormhole intrusion. The safe and proficient method is intended for the separation of malevolent nodes.

4.1 Simulation parameters:

Simulation parameters	Values
Channel – Type	Wireless channel
Propagation model	Two ray groud propagation
Mobility Model	Random way point
Antenna Type	Omi-directional
Number of nodes	100
Speed (s)	150 m/second
Traffic Type	CBR
Mac Type	IEEE 802.11 (b/g)
Routing Protocol	AODV
Area of simulation	800* 800
Time of simulation	100 seconds

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

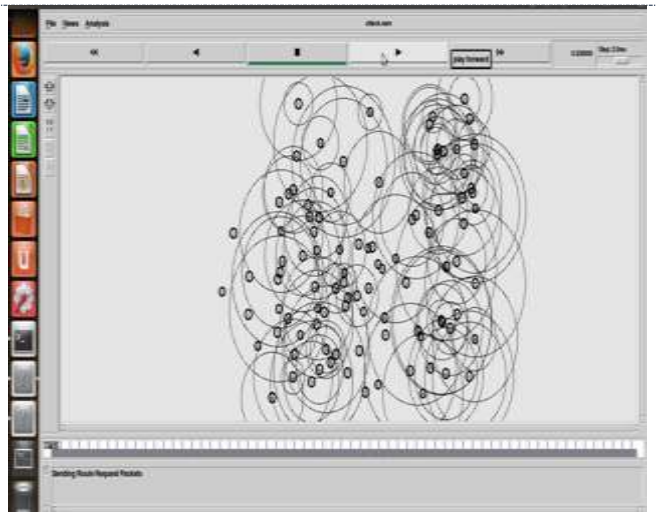

Fig 3: Flooding of route request packets

The MANET is organized in random manner with the fixed amount of movable nodes. MANET is a collection of nodes. These nodes can communicate with each other without using any physical infrastructure. MANET built a temporary network. The source sends the path demand packets in the network for the route creation from one point to other as demonstrated by the figure 3. Then the node which get the path request messages reply back with the path reply messages so that proficient route canbe created from one point to another point as depicted. Then the source node choose the shortet path from source to destination on he basis of the hop count and series number. The source node and destination node establish the communication between them , and then transmit the data between them.

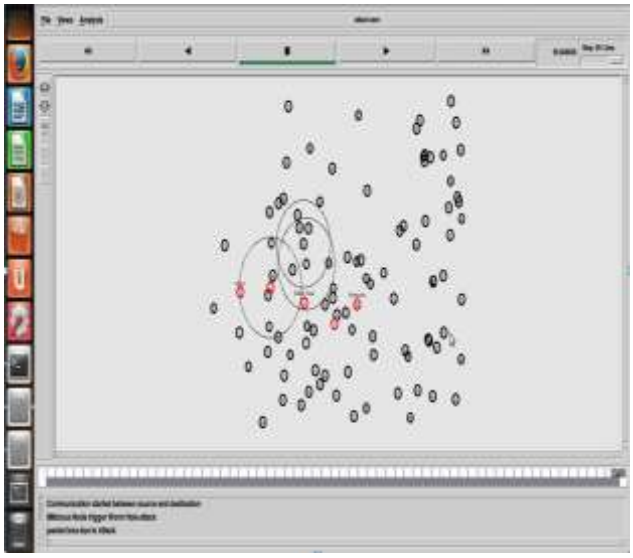

Fig 4: Malicious node

The source node chooses the finest route from source to target according to the hop count as indicated by the figure 4. The malevolent node exists in the route which enhances holdup and launch wormhole intrusion .Because of the wormhole attack packet loss occur or sometime packet reach to the destination node after long time.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

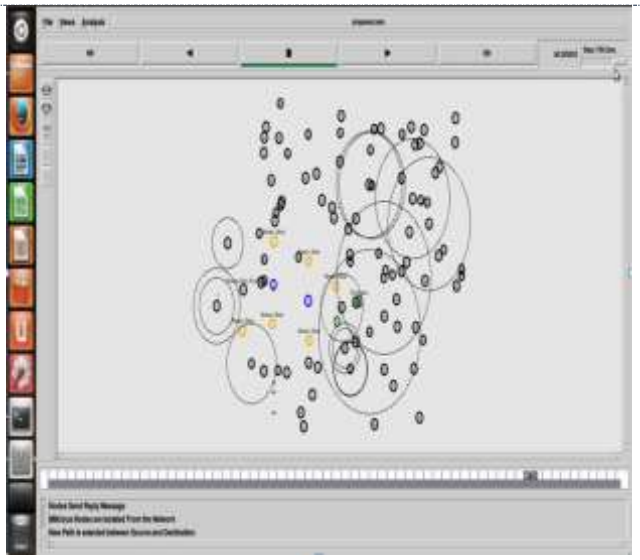

Fig 5: Novel Technique

The route is formed from source to target as demonstrated in the figure 5. The wormhole intrusions are triggered with the help of these attacker nodes in the network. The malevolent node exists in the system increases holdup in the system and packet lost occur. When the holdup in the system increases beyond the threshold level then the new method is implemented for the recognition of malevolent node. A new technique is implemented for the recognition and separation of attacker sensor nodes from the network and it reduce the delay from network.

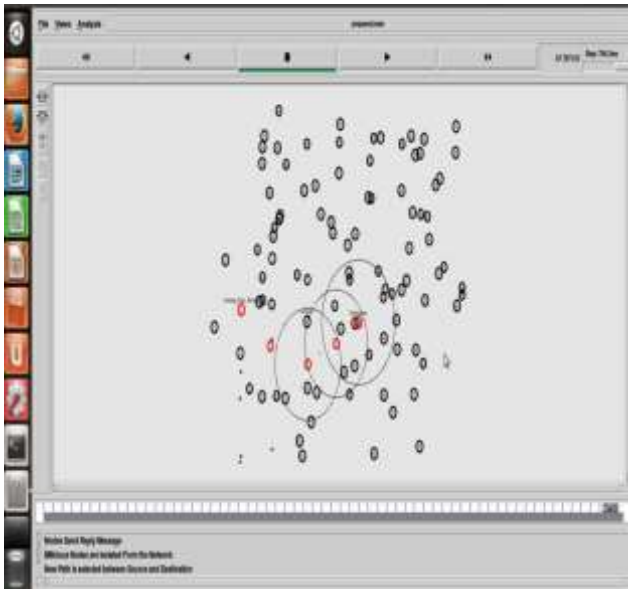

Fig 6: Establishment of Secure Path

When the malevolent node is identified from the system with the help of new method, then novel route is chosen amid source and target for the information broadcasting as depicted by the figure 6. Multipath routing in the network assists in the process of load balancing and reliable delivery during the alternative path when one path fails. Then all data is transmit to the alternative path. Multiple paths can provide load balancing, fault-tolerance, and higher aggregate bandwidth.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

4.2 Result Analysis

Xgraph plotting program is extremely effectual and gives good perfomance when the representation is required in graphic format. With the help of this graph individual can form output files in Tcl scripts by utilizing this graph. These graphs can be used as data suites for Xgraph. In this the results of proposed two phase verification is compared with CREDND scheme in terms of packet loss, energy, throughput for the detection of malicious nodes and the result shows that the proposed work leads greater performance than the existing one.

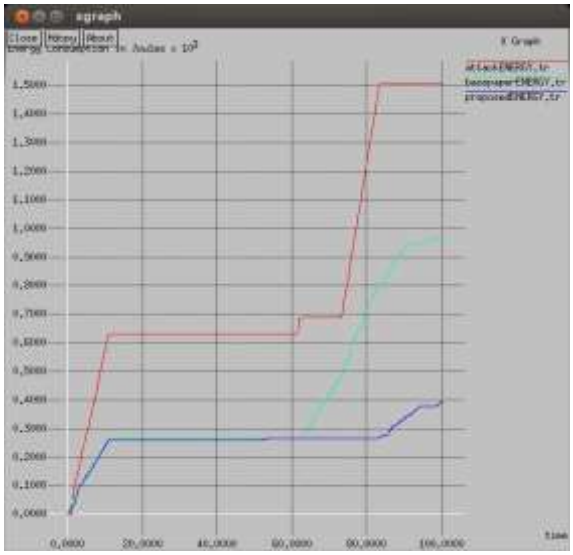

Fig 7: Energy consumption

As shown in figure 7, the power expenditure of intrusion situation, foundation document situation and projected method situation are evaluated for the presentation scrutiny. It is investigated that the projected set-up involves smallest amount of power utilization in comparison with other approaches.

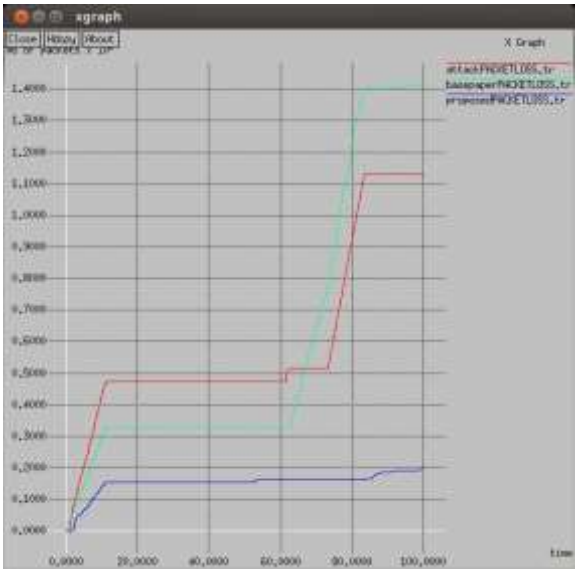

Fig 8: Packet loss Comparison

As shown in figure 8, the package thrashing of intrusion set-up, foundation document set-up and projected set-up are evaluated for the presentation scrutiny. It is scrutinized that package thrashing of projected practice is fewer in comparison with other techniques.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

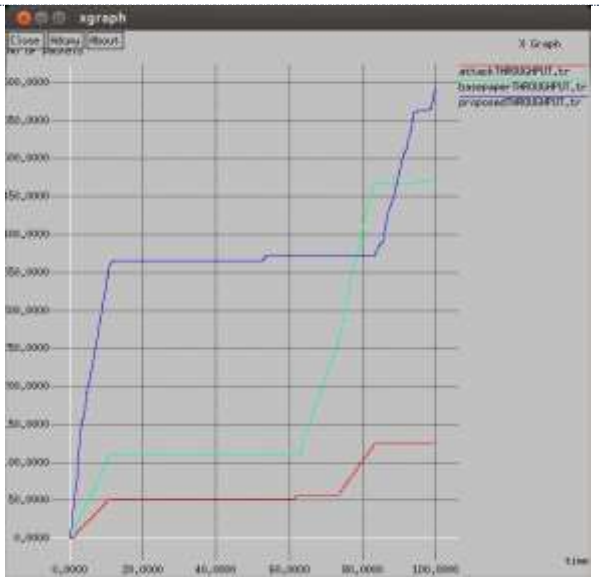

Fig 9: Throughput Comparison

As shown in figure 9, the overall performance of intrusion state, foundation document set-up and projected set-up is evaluated for the presentation scrutiny. It is investigated that overall performance of projected set-up is utmost in comparison with other setups.

5. CONCLUSION AND FUTURE WORK

Conclusion

It is identified that the wireless ad hoc systems are disseminated kind of networks in which sensor nodes can unite or depart the system according to them. No middle regulator is presented in the wireless ad hoc systems. Because of the self reliance character of the system safety, direction finding and service quality are the main problems associated with this system. An active kind of attack named wormhole intrusion may be the reason of the entering of attacker nodes in the system and because of this delay increases. In the presented research, Delphi scheme is utilized. For the recognition of attacker sensor nodes, this scheme shows fewer precision and large implementation times. For the recognition of attacker sensor nodes in the presented study, threshold relied approach is implemented. The projected and accessible approaches are applied in NS2 and the reproduction outcomes depict development in power utilization, overall performance, and package thrashing.

Future Scope

The method utilized in this study can be compared with several other protected methods. The projected method can be auxiliary used to maintain the quality of service of the network.

REFERENCES

[1] M Moharlalpriya and I Krishnamurthi. “Modified DSR protocol for detection and removal of selective black hole attack in MANET”, Comput. Electr. Eng., volume 40, issue 55, pp-530-538. 2014.
[2] VK Sagtani, and SKumar, “Modern Approach to Enhance Routing Recitation in MANET”. International Journal of Emerging Technology and Advanced Engineering, volume 4, issue 7, pp.265-270, 2014.
[3] Y. Hu, A Perrig and D. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on selected areas in communication, Vol. 24, No. 2, pp- 823-836, 2006.
[4] AC.Yao, "Protocol for Secure Computations," in proceedings of the 23rd annual IEEE symposium on foundation of computer science, volume 5, issue 14, pages 160-164, 1982.
[5] D. K. Mishra, M. Chandwani, "Extended Protocol for Secure Multiparty Computation using Ambiguous Identity," WSEAS Transaction on Computer Research, Vol. 2, issue 2, pp- 264-275, 2007.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[6] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining," J. SIGKDD Explorations, Newsletter, VolA, No.2, ACM Press, pages 28-34, 2002.
[7] R. Sheikh, B. Kumar and D. K. Mishra, "PrivacyPreserving k-Secure Sum Protocol," in International Journal of Computer Science and Information Security, Vol.6 No.2, pages 184-188,, 2009.
[8] Sayan Majumder, Prof. Dr. Debika Bhattacharyya, "Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach", 2018, IEEE
[9] Roshani Verma, PROF. Roopesh Sharma, Upendra Singh, "New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017
[10] Pratik Gite, "Link Stability Prediction for Mobile Ad-hoc Network Route Stability", International Conference on Inventive Systems and Control, 2017
[11] Kavitha T, Muthaiah R, " INSTANT ROUTE MIGRATION DURING LINK FAILURE IN MANETS", International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 8, August 2017
[12] Sunil Kumar Jangir, Naveen Hemrajani, "A Comprehensive Review On Detection Of Wormhole Attack In MANET", 2016, IEEE
[13] H.Ghayvat,nb S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap, K.H.Wandra, "Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET", 2016 Tenth International Conference on Sensing Technology
[14] Chitra Gupta, Priya Pathak, "Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET", 2016 Symposium on Colossal Data Analysis and Networking (CDAN)
[15] Kavitha T, Muthaiah R, " INSTANT ROUTE MIGRATION DURING LINK FAILURE IN MANETS", International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 8, August 2017
[16] Roshani Verma, PROF. Roopesh Sharma, Upendra Singh, "New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017
[17] Avni Tripathi, Amar Kumar Mohapatra, "Mitigation of Blackhole attack in MANET", 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), Pages: 437 – 441
[18] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-based secure routing against blackhole attack in MANET", 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Pages: 1960 – 1964
[19] Chanda Dhakad, Anand Singh Bisen, "Efficient Route Selection By Using Link Failure Factor In MANET", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016
[20] Sunil Kumar Jangir, Naveen Hemrajani, "A Comprehensive Review On Detection Of Wormhole Attack In MANET", 2016, IEEE
[21] H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap, K.H.Wandra, "Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET", 2016 Tenth International Conference on Sensing Technology
[22] Chitra Gupta, Priya Pathak, "Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET", 2016 Symposium on Colossal Data Analysis and Networking (CDAN)
[23] Mohamed A. Abdelshafy, Peter J. B. King, "Dynamic source routing under attacks", 2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM), Pages: 174 – 180
[24] S. B. Geetha, Dr. Venkanangouda C. Patil, "Elimination of Energy and Communication Tradeoff to Resist Wormhole Attack in MANET", International Conference on Emerging Research in Electronics, Computer Science and Technology – 2015
[25] HARPREET KAUR, GURBINDER SINGH BRAR, Dr. Rahul Malhotra, "TO PROPOSE A NOVEL TECHNIQUE TO REDUCE LINK FAILURE PROBLEM IN MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 10, October 2014