IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 38, No. 3, June, 2021, pp. 837-843
Journal homepage: http://iieta.org/journals/ts

An Efficient Signal Processing Model for Malicious Signal Identification and Energy Consumption Reduction for Improving Data Transmission Rate

Yaswanth Kumar Alapati*, Suban Ravichandran

Department of Information Technology, Annamalai University, Annamalai Nagar 608002, Tamil Nadu, India

Corresponding Author Email: aykumar@rvrjc.ac.in

https://doi.org/10.18280/ts.380330

Received: 17 March 2021
Accepted: 5 June 2021

Keywords:
malicious signal, data transfer, routing, data loss, congestion control, signal behavior, data delivery rate, energy consumption

ABSTRACT

One of the fields which needs the most security is Ad hoc Network (ANET). The term ANET guarantees that there is no central authority so as to administer the signals. Security is a basic issue while using ANET for establishing communication. A ANET is an assortment of remote signals that can progressively be set up at anyplace and whenever without utilizing any prior system framework. Because of its volatile nature, it has mobility issues to improve the arrangement of the system. One of the difficulties is to recognize the malicious signals in the system. Because of malicious signals, data loss or high energy consumption will occur which reduce the overall performance of the ANET. There are a few circumstances when at least one signal in the system become malevolent and will destroy the limit of the system. The point of this work is to recognize the malignant signals quickly to avoid loss of data. The conventional strategy for firewall and encryption isn't adequate to secure the system. In this way a malicious signal identification framework must be added to the ad hoc network. A signal needs to be secured when utilizing the resources and to provide secure communication. The ad hoc networks have several issues like, congestion, overload, data loss and energy consumption. In the proposed work a framework for Rapid Malicious Signal Detection with Energy Consumption Reduction (RMSDwECR) Method is proposed. The proposed method is compared with the traditional methods in terms of load in the network, data loss ratio, signal transmission rate, energy consumption levels, malicious signal identification time and throughput levels. The proposed method exhibits better performance than the traditional methods.

1. INTRODUCTION

ANETs assumes a critical job in circumstances where there is a requirement for fast arrangement of communication during natural disasters or in conditions where fixed network is failed [1]. ANETs have a significant application in military war zone, where a fixed framework is beyond the area of imagination and couldn't be followed. These systems imagine to help an ever increasing number of utilizations than only for structuring a communication medium [2]. Ad hoc network is an assortment of versatile signals, which frames a transitory system without the need of central authority or standard gadgets routinely accessible as ordinary systems. These signals by and large have a constrained transmission run and thus, every signal looks for the help of its neighboring signals in sending signals and consequently the signals in an Ad hoc system can enter or leave the network at any time [3].

In this manner a signal may transmit data bundles between different signals based on the routing table. Naturally these kinds of systems are appropriate for circumstances where either no fixed framework exists [4]. ANETs have discovered numerous applications in different fields like military, crisis, conferencing and sensor systems [5]. Every one of these application territories has their particular prerequisites for performing routing process [6]. The routing conventions for

ANETs can be comprehensively arranged into four classifications dependent on routing data update components. The structure of ANET is depicted in Figure 1.

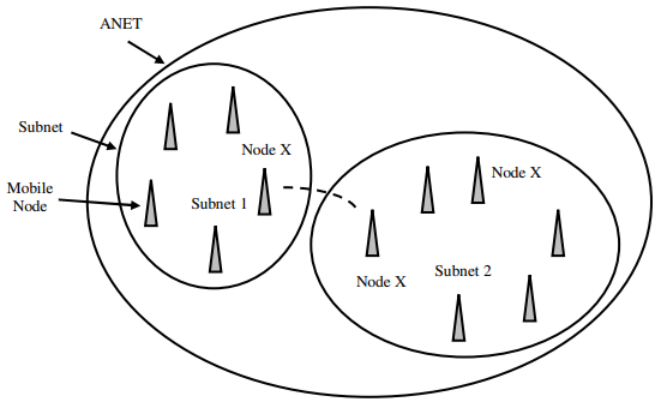

Figure 1. ANET architecture

In ANETs, every single moving signal arranges among themselves to empower communication and to oversee routing and resources; this is done in a circulated way [7]. This implies every signal in the ANET must be increasingly smart, with the goal that it can work as a sender for transmitting messages, can get information from another signal that got the first message, and can act as a switch for sending data to different signals [8].

ANETs work in an extremely unique and circulated nature, and signals are for the most part battery fueled and have a restricted force. Energy utilization is a key issue in ANETs, once in a while causing failures in a signal that can influence

the entire system [9]. Energy effective approaches to decrease the utilization of system energy and to identify the malicious signals need to be considered for example, reporting the rest of the energy level of a signal and signal transactions for malicious signal detection which will maintain a strategic distance from consumption of energy and reduce the loss of data [10].

The ad hoc network is one area that needs improved security as these kind of networks are frequently used. The Ad-Hoc Network is a transient, wirelessly connected network with no fixed infrastructure made of nodes [11]. Network security plays a key role here and is no longer effective and sufficient in traditional approach to ensure network protection through firewalls and encrypted software [12]. Sensitive information can be shared in the ad hoc networks, so care need to be taken to provide security to the data from attackers or malicious signals that degrade the performance levels [13]. Mechanisms for malicious signal detection should be developed to provide the ANET with enhanced security [14].

For several reasons, the ad-hoc network presents several issues in security. They are:

- The wireless network is especially susceptible to attacks due to passive interference.
- It's incredibly hard to adopt and apply security solutions because of the absence of Trusted Third Party.
- The computing and power consumption functions mostly nodes are restricted and more exposed to Denial of Service attacks.
- Heavy security techniques, such as publicly available key algorithms, are not also feasible [15].
- Due to the less and more self-organizing qualities of ANET, there are greater chances to compromise confident nodes and launch network attacks or malicious signals [16].
- Due to the node mobility mechanism, it is impossible to differentiate between stale routing and bogus routing information and also in identifying normal or malicous signals.
- It frequently re-configures the networking process in node mobility mechanism, creating more opportunities for attacks.

The information transmission starting with one signal to another signal or any sort of transmission of information depends on the availability of the system signals. In ANET, the availability is constantly a multifaceted issue because of system topology [17]. The availability between two signals in a ANET is totally unique compared to a wired system. The neighboring signals consistently continue changing in a ANET though in the wired system they stay steady. In light of this explanation, the routing also assumes a significant job for availability of the system.

The main issue in ANET routing conventions comparing to the undermined signals is the involvement of malicious signals that decrease the network performance [18]. Here, the malicious conduct of signals can't be legitimately noted, since the malignant signal can be transmitted to nodes as a normal signal and then it performs malicious operations in the network [19]. Subsequent to data transmission, the malignant signal makes new routing messages, promotes non-existent connection, offers inaccurate connection data and causes different signals with routing traffic, and therefore causing the loss of the data thereby decreasing the system performance.

The ANETs need greater security since they are increasingly helpless against attacks by structure. The utilization of remote connections makes a ANET increasingly powerless to attacks going from uninvolved intelligence work to dynamic interfering [20]. When contrasted with a wired system, it is simpler to attack a remote system on account of its structure and the attack may come towards any path and any signal can be attacked anytime. Along these lines, every single signal in the system needs to plan for attacks anytime. And furthermore as there is no focal based controlling administrator for the taking action on signals. The attacks are a lot simpler to transmit in ANET. The key necessities for ANETs are privacy, verification, trustworthiness, Authorization, originality, non-renouncement and accessibility.

2. LITERATURE SURVEY

The open peer-to-peer architecture is one of the core vulnerabilities of ANETs. There will be dedicated routers on wired networks, but each ad hoc node is used for routing in ad hoc networks so that signals can be sent to nodes. There are no wireless channels in ad hoc networks; both network users and malicious attackers have access to this. There is therefore no clear line of defense for security design in ANET networks. The line that is utilized to distinguish the intern network from the external network becomes hazy. As a result, no well-defined infrastructure is available to deploy a single ANET security solution.

Pathan et al. [1] developed a justifying routing mismatches in multi-faceted systems, with two approaches aimed at improving performance in a specially designated system for signals that allow for the transmission of signals. To mitigate this problem, the watch dog technique identifies the removal of malicious signals rather than helps to stay away from them. By redefining the watch dog evaluate the way the signal is transmitted, the overall transmission level and the accuracy of the signal finding. As portable remote systems with different features from wired and even distant standard devices, the suggested Enhanced intrusion Detection Systems for the Discovery of Malicious Signals in Mobile Ad Hoc Networks has additional, security-related inducements to be recognised. Many frameworks were developed for intrusion-discovery and most of them were strongly identified with routing agreements, such as the Watchdog/Route and Route monitors. The arrangements include two areas: the finding of interruption (watchdog) and the reaction (Path rater and Route monitor). Watch a dog lives in all signals and is connected to it.

Gurung and Chauhan [3] proposes a Rough Set Based Approach to Classify Signal Behavior in Mobile Ad Hoc Network, there are a few circumstances when at least one signal in the system become harmful and will in general destroy the limit of the system. This examine the arrangement of good and terrible signals in the system by utilizing the idea of rough set hypothesis, that can be utilized to produce basic guidelines and to evacuate immaterial qualities for recognizing the great signals from awful signals.

ANET detection for data dropping signals using the DSR routing protocol is portrayed by Tiruvakadu and Pallapa [4]. The methodology is used to detect malicious neighbouring ideal signal checks. Every signal will not be an inspection signal, however, on the grounds that each signal has battery power restrictions on the portable specially-defined system, so

that each signal should not be in listening mode, it will decrease administration time. These observational signals recognise the data drop signals in the area and preserve confidence data on every signal of the area, and they provide the source signal with the same data as other inspection signals at any necessary point.

Gurung and Chauhan [5] have established a calculation for the identification of harmful signals in ANET attacks. In order to determine the specific placement of malicious signals in ANET conditions, the authors used the Cluster Head Switch (CGS) standard. A strategy used to identify and weaken ANET hazardous signals is proposed by Hammamouche et al. [7]. Schweitzer et al. [8] methodology is used to recognise harmful signals in ANET. In the system condition the authors analysed signal misconduct and boycotted the unified signal. In their test, the creators used 90 signals. If the number of harmful signals was high, the calculation would be short.

Gupta [10] utilized LEACH convention to bunch the self organizing signals. The cluster heads were arbitrarily chosen and this determination depended on most noteworthy energy levels. The previously mentioned chosen cluster head performs information combination for packing the information, subsequently expanding the throughput and system life time. The whole information on the system isn't fundamental right now group the signals in the remote condition.

Sandhya Venu and Avula [12] introduced a Secure Objective Reputation Based Incentive (SORI) framework which controls the malicious signals. Their technique comprised of neighbors checking the neighbor signals for their signal sending conduct and a neighbor signal list comprising of complexity of all the neighbor signals are being kept up by every signal in the framework. All the signals share messages to recognize the malicious signal. After malicious signals are identified, a discipline scheme is actualized to remove the malicious signals. An uncommon element of their system is that behavior is made sure about by one way hash based confirmation scheme and less communication overhead because of spread of disrepute just among the neighboring signals.

Arulkumaran and Gnanamurthy [14] developed an approach that rely on ignoring the key route to reducing the black-hole attack's aggressive effects. The first RREP message expected would usually come from a malevolent signal. Shockingly, there are a few constraints on this arrangement. For example, when the original destination signal is closer to the source signal than the malicious message, the second RREP message received may be from the malicious signal as well. In addition, this methodology does not allow harmful signals from the system to be recognised and separated.

Taha et al. [16] offered a methodology reliant on the link between the signals that would lead to a particularly designated situation in which they participated. The confidence estimation is determined by the trust units of each signal in the system. By using the trust values determined, the relationship estimator estimated the relationship status of signals. Their suggested upgrade is contrasted with the standard DSR practise and the results by using Network Simulator 2.

3. PROPOSED METHOD

The security is the essential issue in ANET which reduces the system execution fundamentally if there are any malicious activities happened in the ANET. In the proposed work a Rapid Malicious Signal Detection with Energy Consumption Reduction strategy is proposed to identify and evacuate the noxious signals. Every signal inside the ANET gets updated information from the Head signal which is considered as Malicious Signal Identification Mode (MNIM) and this information is utilized for identification of malicious actions during the data communication. Malicious signal discovery and removal is a challenging issue in ANETs because of comparable attributes with trusty signals in the detecting zone. The proposed Rapid Malicious Signal Detection Method continuously verifies the updated routing information and monitors the signals involved in the routing process and assigns a Unique ID vectors for the signal after forwarding the signals to the neighbors. The proposed method is named as Rapid Malicious Signal Detection because, MNIN signal assigns Unique ID for every signal after successful data transmission and monitors the signals continuously until the data reaches the destination successfully without data loss and removes the malicious signals when identified.

Let {UID1, UID2…} be the underlying Unique ID vectors of the signals {n1, n2…} along the route R from a source S to the Destination D. Since the signal doesn't have any data about the dependability of its neighbors to start with, signals can be completely trusted nor be completely doubted. At the point when a source S needs to send data to the Destination D, it sends ACK message to the MNIN signal which is a part of the network. The MNIN signal verifies the routing information and checks whether the message is received from genuine Source S. If the signal S is genuine, then communication is initiated. The MNIN assigns a Unique ID vector for every signal after successfully transferring the data to the neighbor signal.

The process of calculating Unique ID Vector is as follows:

Signal set = {N1, N2,……Nn}

Unique ID(Ni) = Sender Address+K+ TI

UID(Ni) = Unique ID(Ni)+Destination Address.

UID(Ni+1) = UID(Ni) ε {1 to 200} && UID(Ni+1) != UID{Prev}

Update UID(Ni(n))

where, N is the Signals in the ANET, K is the constant, TI is the time instance. Prev is the previous Unique ID vector.

The normal estimation of transmission measurements are considered so as to group the signals dependent on the Unique ID Vectors. The malicious signals of system are recognized and removed from the routing by the MNIN signal and a rerouting process in initiated. The refreshed routing table is updated for routing process in routing table. The proposed technique is utilized to recognize the malicious signals in the system.

Step-1: Establish a ANET with at least 50 Signals.

Step-2: To discover the transmission measurements of a signal, for example,

Data Delivery Rate (PDR) = No. of signal data received/No. of sent signalsX 100

End-to-End delay: = Received Time – Data Send Time/No. of Connections

Throughput = Received Data beginning time − stop time X 50/100

Data Lost Rate (PLR) = Received Signal – Transmitted Signal

Select a MNIN signal from the routing table which has high energy levels.

Step-3: After route is identified, MNIN signal is selected among the route which assigns a ID to all the signals in the routing table.

Step-4: MNIN signal calculates Unique ID Vector and assigns for each signals involved in communication. The similarity between two neighbors is identified as:

$$Sim(X,Y)=\sum ti(X)\in N(TS)+\sum ti(Ni+Y)\in N(v)(I(t))-1$$

Here X and Y are considered as 2 signals of the nodes. The frequency levels and signal strength model is used to identify the similarity difference among those signals to distinguish normal or malicious signals. The time instance of the signals ti is also considered and checked whether the signal transmitted is exactly transmitted to the other nodes.

Step-5: MNIN signal verifies the data transmission rate of each signal and if any signal data transmission is less than 80%, then it is marked as Malicious signal and removed from routing process.

Step-6: Unique ID vectors are identified and used for further communication to differentiate malicious signals and normal signals.

Step-7: Remove the malicious signal and initiate rerouting process and update the routing table.

3.1 Energy consumption reduction methodology

When a ANET is established, initially all signals are allotted with a specific energy level. Based on the operations performed by the signal, its energy consumption depends. If a network has malicious signals, the energy consumption of the network is high as the malicious signals intentionally consumed more power. The energy consumption of the signals in the ANET need to be avoided for better throughput of the network. In the proposed method, a Start/Stop technique is utilized for avoiding the signals to consume the power continuously. The proposed method allows the signals to consume power only when it receives the data and in remaining conditions, the signal enters into blocked state which does not consume any energy. The signal when in start stage, it submits the ID to the MNIN signal for authentication. If the signal is a valid signal, the data is communicated to the neighbor signal. The MNIN signal updates the IDs of the signals in regular time intervals.

Algorithm: ECN Method

{

Step-1: Create a ANET.

Step-2: Perform Route Identification Process.

Step-3: Assign specific energy levels in joules to all signals in routing table.

Step-4: Identify the Status of the battery.

For all signals in ANET

{

if(Remaining battery charge>=25)

{

Receive the data from the sender and forward to next neighbor.

Enter into block stage for T time interval. (T is the threshold time set)

if (T is reached)

{

Enter into Start Stage.

}

else

{

Check the signal status by sending VERIFY message to MNIN Signal.

If (Signal id valid)

{

Assign M power level. (M is the specified additional Power level)

}

else

{

Remove the signal and restart the routing process.

}

}

}

}

Step 5: Calculate energy consumed by every signal

Energy consumed (EC) = Transmitting Current * Voltage * Time

Remaining Energy Level (REL) = Alloted Energy – Present Energy.

If (REL>25)

{

Continue until communication is completed.

}

Else

{

End the communication

}

}

The proposed energy consumption reduction method effectively reduces the energy consumption of the signals by limiting the signals to consume the energy for a particular time interval. As the energy consumption level is reduced the performance of the network can be increased.

4. RESULTS

The proposed method uses a NS 2.35 simulator for establishing a network and performs identification of malicious signals. The proposed method is compared with the traditional methods in terms of malicious signal identification time in milliseconds, data loss rate in terms of packets, signal Transmission ratio in terms of strength, Energy consumption levels in joules, congestion control. The parameters used in the proposed work are depicted in Table 1.

The proposed model uses NS2 in ubuntu and the process of creating experimental setup is indicated in Figure 2.

The process of executing the tcl scripts created to establish a ANET is indicated in Figure 3.

The proposed method establishes a ANET in which source can send information to destination signal using MNIN signal and ECN signal by reducing energy consumption reduction and removing malicious signals in the ANET. The ANET is depicted in Figure 4.

Table 1. Parameters used

Simulation Parameter	Value
NS2 Version	Ns-allinone-2.35
Simulation area	2000 m X 800 m
Antenna Type	Omni Antenna
Initial Energy	1000 joules
Queue Length	64
Data rate	Variable
Radio Range	~250 m
Mobility Model	Random way point
Mobility Speed	1.5 ms

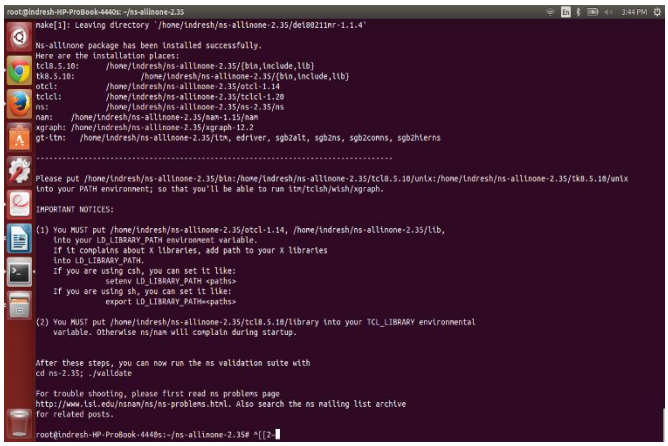

Figure 2. Experimental setup

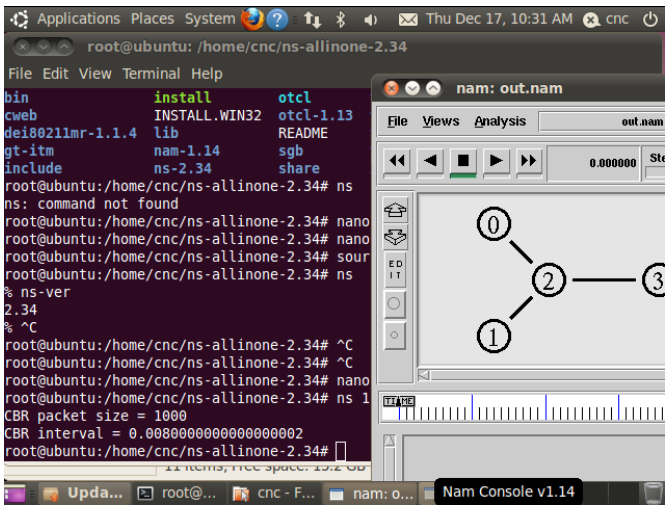

Figure 3. TCL script execution

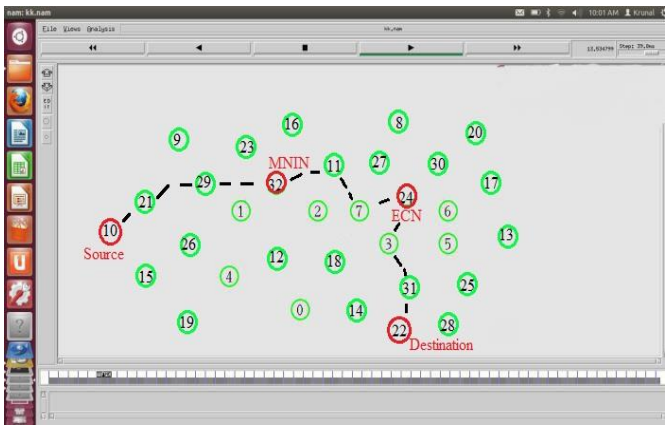

Figure 4. ANET created

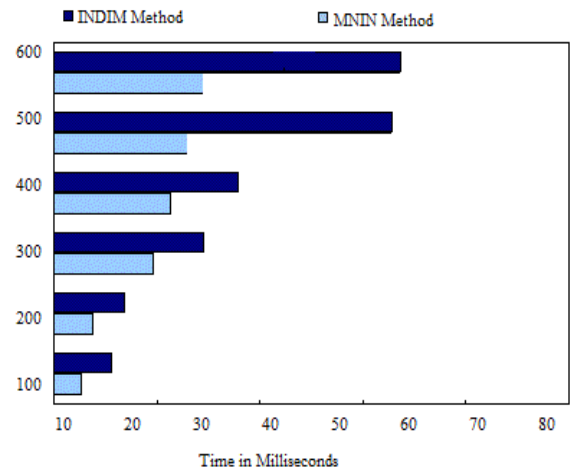

Figure 5. Malicious signal identification time

The proposed Malicious Signal Identification Signal (MNIS) method is compared with the traditional Intruder Signal Detection and Isolation Method (INDIM) and the results depicts that the time taken for identification of malicious signals in the proposed method is less than the traditional method. The proposed model is compared with the INDIM model for achieving better results as the existing model also proposed a framework for detection of malicious actions in ad hoc networks. The existing models fails to achieve better accuracy rate in malicious actions detections and the performance levels are also poor. Figure 5 represents the time levels for identification of malicious signals in the ANET.

The proposed method provides better security for the data communicated in the network and the method identifies the malicious signals in the network. The Data Drop rate of the proposed method is less when compared to the traditional methods. Figure 6 represents the data drop rate of the proposed and existing methods.

The proposed method provides better security for the data communicated and avoids malicious signals in the network by monitoring all the signals in the network. The Data Delivery Rate of the proposed method is high when compared to the traditional methods. Figure 7 represents the data delivery rate of the proposed and existing methods.

The Congestion Level of the proposed method is less as the MNIN signal rapidly monitors all the signals in the ANET. The energy consumption can be effectively reduced if the congestion in the network can be managed. The congestion levels of the proposed method and the traditional methods are depicted in Figure 8.

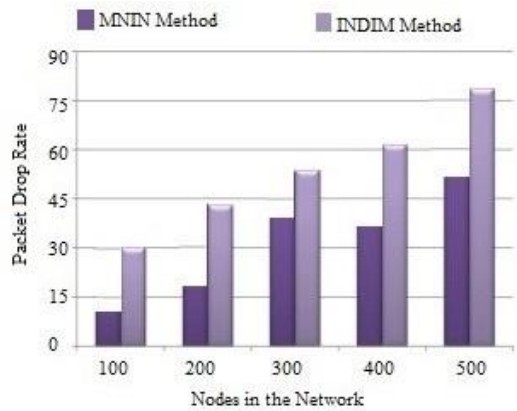

Figure 6. Data drop rate

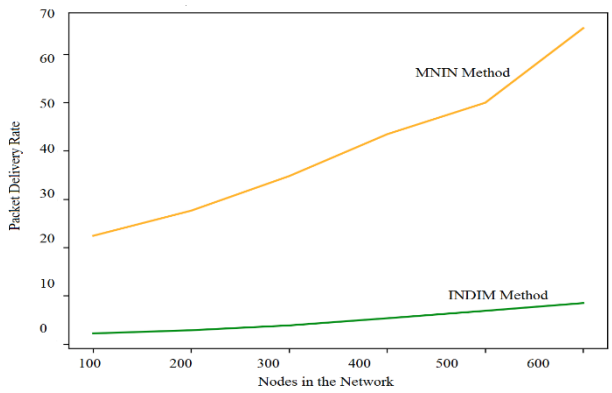

Figure 7. Data delivery ratio

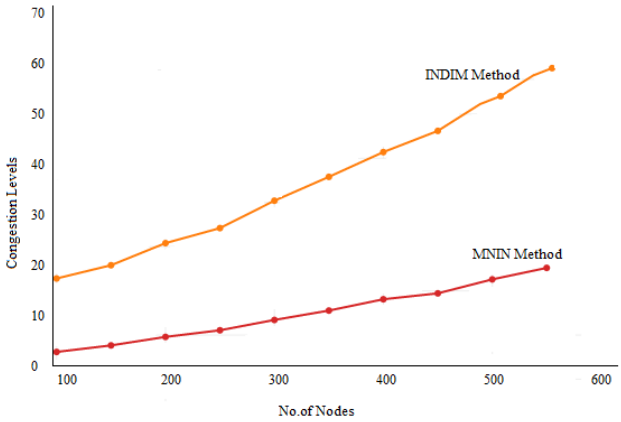

Figure 8. Congestion level

The energy level consumption in the proposed method is less than the traditional method. The Energy Calculator Signal (ECN) calculates the energy consumption of every signal and then balances the load of every signal and makes the performance of the network better. The Figure 9 represents the energy consumption levels of the proposed and traditional methods.

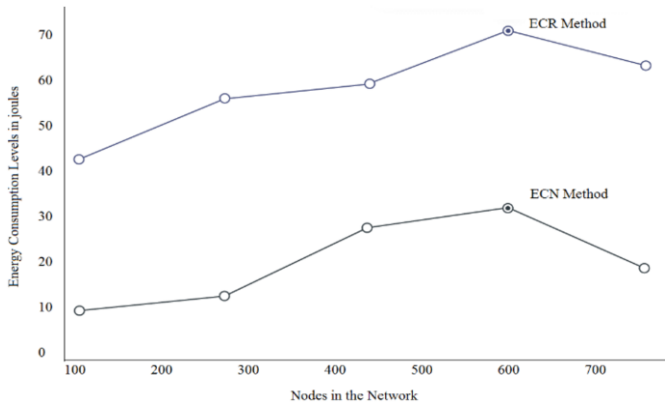

Figure 9. Energy consumption levels

5. CONCLUSION

ANETs has a number of issues to confront. As all nodes are free to join and exit the network and communications, safety was the most critical task in ANET. ANET security and network layer problems must be taken seriously. Network layer faces not only conventional attacks, but ANET-specific threats that are not straightforward to manage with existing protocols in an open communication environment. This safety method should be designed to ensure that harmful signals may be detected and prevented while simultaneously maintaining all ANET's features. The major problem with ANET is that the central administrator is not available. Communication packages need coordinated effort between signals grouped by the mechanism of routing. Data transfer and overall data transfer rate are used to track the harmful signals on the Network during communication. The building of the framework for safe data exchange in particular is one of the major concerns in an ANET's energy expertise. As the signals work based on energy supplies, the energy usage at ANET must be monitored. The suggested methodology recognises harmful signals efficiently in the network and decreases the loss of data and enhances system performance by reducing energy consumption also. In all aspects, the performance of the suggested method is improved. For performance improvement, in the future, the signal parameters and collision reduction can be addressed.

REFERENCES

[1] Pathan, M.S., Zhu, N., He, J., Zardari, Z.A., Memon, M.Q., Hussain, M.I. (2018). An efficient trust-based scheme for secure and quality of service routing in MANETs. Future Internet, 10(2): 16. https://doi.org/10.3390/fi10020016

[2] Roshani, P., Patel, A. (2017). Techniquesto mitigate grayhole attack in MANET: A survey. In 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-4. https://doi.org/10.1109/ICIIECS.2017.8276064

[3] Gurung, S., Chauhan, S. (2019). Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. Wireless Networks, 25(3): 975-988. https://doi.org/10.1007/s11276-017-1639-2

[4] Tiruvakadu, D.S.K., Pallapa, V. (2018). Honeypot based black-hole attack confirmation in a MANET. International Journal of Wireless Information Networks, 25(4): 434-448. https://doi.org/10.1007/s10776-018-0415-2

[5] Gurung, S., Chauhan, S. (2018). A novel approach for mitigating gray hole attack in MANET. Wireless Networks, 24(2): 565-579. https://doi.org/10.1007/s11276-016-1353-5

[6] Khamayseh, Y.M., Aljawarneh, S.A., Asaad, A.E. (2018). Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. Sustainable Computing: Informatics and Systems, 18: 90-100. https://doi.org/10.1016/j.suscom.2017.07.001

[7] Hammamouche, A., Omar, M., Djebari, N., Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. Journal of Information Security and Applications, 43: 12-20. https://doi.org/10.1016/j.jisa.2018.10.004

[8] Schweitzer, N., Stulman, A., Margalit, R.D., Shabtai, A. (2016). Contradiction based gray-hole attack minimization for ad-hoc networks. IEEE Transactions on Mobile Computing, 16(8): 2174-2183. https://doi.org/10.1109/TMC.2016.2622707

[9] Liu, Q., Yin, J., Leung, V.C., Cai, Z. (2013). FADE: Forwarding assessment based detection of collaborative grey hole attacks in WMNs. IEEE Transactions on Wireless Communications, 12(10): 5124-5137. https://doi.org/10.1109/TWC.2013.121906

[10] Gupta, J. (2017). Improved approach of co-operative gray hole attack prevention monitored by meta heuristic on MANET. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 356-361. https://doi.org/10.1109/ISPCC.2017.8269703

[11] Pal, S., Sikdar, B., Chow, J.H. (2016). An online mechanism for detection of gray-hole attacks on PMU data. IEEE Transactions on Smart Grid, 9(4): 2498-2507. https://doi.org/10.1109/TSG.2016.2614327

[12] Sandhya Venu, V., Avula, D. (2018). Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks. International Journal of Communication Systems, 31(6): e3518. https://doi.org/10.1002/dac.3518

[13] Tamilselvi, P., Babu, C.G. (2019). An efficient approach to circumvent black hole nodes in Manets. Cluster Computing, 22(5): 11401-11409. https://doi.org/10.1007/s10586-017-1395-1

[14] Arulkumaran, G., Gnanamurthy, R.K. (2019). Fuzzy trust approach for detecting black hole attack in mobile adhoc network. Mobile Networks and Applications, 24(2): 386-393. https://doi.org/10.1007/s11036-017-0912-z

[15] Gopinath, S., Kumar, K.V., Sankar, T.J. (2019). Secure location aware routing protocol with authentication for data integrity. Cluster Computing, 22(6): 13609-13618. https://doi.org/10.1007/s10586-018-2020-7

[16] Taha, A., Alsaqour, R., Uddin, M., Abdelhaq, M., Saba, T. (2017). Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function. IEEE Access, 5: 10369-10381. https://doi.org/10.1109/ACCESS.2017.2707537

[17] Smail, O., Cousin, B., Mekki, R., Mekkakia, Z. (2014). A multipath energy-conserving routing protocol for wireless ad hoc networks lifetime improvement. EURASIP Journal on Wireless Communications and Networking, 2014(1): 1-12. https://doi.org/10.1186/1687-1499-2014-139

[18] Manickavelu, D., Vaidyanathan, R.U. (2014). Particle swarm optimization (PSO)-based node and link lifetime prediction algorithm for route recovery in MANET. EURASIP Journal on Wireless Communications and Networking, 2014(1): 1-10. https://doi.org/10.1186/1687-1499-2014-107

[19] Sun, B., Gui, C., Liu, P. (2010). Energy entropy multipath routing optimization algorithm in MANET based on GA. In 2010 IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), pp. 943-947. https://doi.org/10.1109/BICTA.2010.5645139

[20] Hu, X., Wang, J., Wang, C. (2011). Mobility-adaptive routing for stable transmission in mobile Ad Hoc networks. JCM, 6(1): 79-86. https://doi.org/10.4304/jcm.6.1.79-86