Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A Performance Enhancement and Optimisation of the Secure Channel for Application in MANET Routing Protocols

D. Naga Tej[1*], K V Ramana[2]
Research Scholar, JNTUK, Kakinada and Assistant Professor, Gayatri Vidya Parishad College of Engineering, Madhurawada, Visakhapatnam Andhra Pradesh, India[1]
Professor, JNTUK Kakinada, Kakinada, Andhra Pradesh, India[2]

Article Info

Page Number: 4749 - 4761

Publication Issue:

Vol 71 No. 4 (2022)

Article History

Article Received*: 25 March 2022*

Revised*: 30 April 2022*

Accepted*: 15 June 2022*

Publication*: 19 August 2022*

Abstract

Sensor networks are increasingly being used for a wide variety of purposes, prompting academics to develop a variety of approaches to this problem. Sensor networks have minimal limits to improve the network's performance. The network architecture and energy efficiency are the two major stumbling blocks for the systems' performance. The topologies of sensor networks are not constrained by any design and are dynamically altered by device mobility. In addition, since the gadgets are battery-powered, the algorithms have to be cognizant of power consumption. There are barriers in the research to enhancing performance because of these constraints. A good deal of work has been done to increase performance, focusing on better routing. Despite this, it is impossible to ignore the present algorithms' energy efficiency. Since then, researchers have been looking for a routing algorithm that is both efficient and energy conscious. A new route-optimized cluster-based algorithm with low energy usage results from this research.

Keywords— Tactical Sensor Network, Cluster-based, TEEN, SEP, EAMMH; Optimal Route, Energy Awareness

1. Introduction

Routing in a Mobile Ad hoc Network (MANET) is essential, and it should be done quickly before a node departs the network. A friendliness and ease of use are the primary goals of MANET routing methods, making them vulnerable to various assaults. One of the most promising areas for remote system innovation is MANET. MANET has become one of the most active and energetic fields of communication among systems. A MANET is a self-sufficient group of mobile nodes that communicate with each other through distant connections and coordinate in an appropriate manner so that the core system may operate without the need for a fixed network infrastructure. Although MANET's transmission speeds are limited, it allows flexible clients to communicate independently across it. After some time, the system's architecture becomes unpredictable due to the frequent movement of nodes and the resulting changes in route topology. Decentralization requires safe route identification among nodes in order to facilitate communication. Route discovery can only be carried out with trustworthy nodes once a trust calculation has been completed. The changing topology of the network necessitates regular updates to the routing table, which is why this paper proposes a new safe routing mechanism that uses route identification between trustworthy nodes. Comparison with other approaches shows that our approach utilises a superior routing methodology [1].

MANET is becoming more necessary in today's world of wireless networks. The wide range of mixed media applications operating in an infrastructure-less situation is the explanation for this widened scope of analysis. Because of the changing topology, power constraints, and lack of a framework in MANETs, it is very difficult to provide a safe and secure environment. An introduction to different types of assaults and defence mechanisms is provided in this paper. A brief

comparison of several protocols for anchored routing in MANET is also provided, as well as an explanation of the essential properties of MANET.

A MANET is a kind of wireless mobile network that may be set up with minimal infrastructure requirements. Such networks allow each node to function as a router, and each node is capable of doing so. The topology of a MANET may be described as dynamic since the nodes in the network can join and depart at any moment owing to their mobility. The research community has recently placed a high priority on MANET security. MANETs are the target of a wide variety of assaults, but the solutions to these problems have received little attention in the literature. In wired networks, there are a number of options for addressing security concerns, but the same cannot be said for wireless networks. Many MANET routing systems have been developed, however most of them function poorly when malicious nodes are present. A novel hybrid secure routing protocol (S-DSR) is the subject of this research, which may increase the ratio of packets delivered and the rate at which they are processed by nodes in the network. The trust information from the neighbouring nodes is used to determine the optimum route for safe file transfer in this protocol. On NS-2, the suggested protocol has been tested and is working as expected. In terms of packet delivery and latency, this protocol outperforms other protocols like AODV, AOMDV, etc. [3].

2. Recent Research Reviews

Because of its broad relevance in fields like military, implementing security in MANETs has been a difficult and contentious research issue over the last two decades. There have been several attempts in this approach. This issue may not be entirely resolved by the current set of security algorithms, methodologies, models, and frameworks. This paper analyses a security for the Ad hoc on-demand distance vector (AODV) reactive routing protocol as a security solution based on an outlier detection system. It is a defense against the Blackhole attack in mobile ad-hoc environments, and it was inspired by a variety of current security mechanisms and anomaly detection. The simulations conducted using the network simulator tool demonstrate that the proposed algorithm is more straightforward, more robust, and more successful than both the original AODV protocol and the existing approaches [4].

The increase in mobile devices has led directly to the growth of mobile ad hoc networks (MANETs). MANETs are simple to construct since they do not need infrastructure and are dynamic. It is feasible for an attacker to conduct an attack by exploiting the open nature of MANET and the absence of centralized control and oversight. It is possible to conduct attacks against all wireless networks. RREP is the protocol utilized to provide a forged route reply (RREP) to the destination. Likely, routing protocols such as AODV and DSR will not function properly if this node is absent from the network. According to the research available, the protocols of MANETs are not intended to identify nodes or paths that black holes have compromised. As a result of this observation, the researchers suggest a DSR-based safe routing technique for recognizing black hole attacks. Within the context of the suggested method, a validity value is given to RREP. At the first intermediate hop, along with the route reply, this validity value is validated, and a check to guarantee there is no black hole attack is done [5].

The military and civilian sectors both use Mobile Ad hoc Networks. AODV, DSR, and other MANET routing protocols presume that nodes be trustworthy and cooperative. These assumptions make it easier for DDoS attacks of different kinds to penetrate wireless ad-hoc networks and get access to the data sent over them. This paper proposes a reputation-based safe routing technology to reduce the impact of rogue nodes. There are 25 nodes in a 55 grid, which is the core notion of the suggested method. In the network, each normal node is identified by a unique prime number. It is arranged in a 5x5 grid with a Backbone Network (BBN). The suggested system makes advantage of a backbone network's legitimacy value and reputation level tables. After avoiding potentially harmful nodes during route finding, these tables are utilised to offer the optimum path selection.

While traversing the network, the nodes' legitimacy table and reputation level tables help them to identify and avoid hostile nodes.

The adoption of mobile devices and the growth of ad hoc networks for mobile devices are occurring rapidly in MANETs. MANETs are adaptable and simple to set up since they self-configure, do not depend on external infrastructure, and can be built practically anywhere. MANET is susceptible to active attacks, such as black holes, due to the absence of centralized management and coordination. Additionally, black hole attacks may be performed against mobile ad hoc networks and wireless sensor networks. When a black hole collides with a node, it falsely asserts that it has the quickest and most direct path to its destination, luring other ships to follow it. In a network including such a node, there is a risk that routing protocol issues may arise. The most extensively used MANET protocols, such as ADOV and DSR, cannot defend against a black hole attack or a route impacted by a black hole. As a result, the paper provides an AODV-based safe routing strategy that can detect and eradicate both black hole attacks and impacted routes in the early stages of route discovery. The RREP validity value assures that the route is safe and cannot be attacked. Simulation in NS2 [7] is necessary to assess the provided method's effectiveness.

It is a self-organizing and infrastructure-free network. Multiple nodes offer a temporary infrastructure for establishing connections and exchanging information between nodes in this system. Black hole is one of several probable assaults, according to MANET nature. Several different routing structures are used by MANET. Routing protocols such as AODV are dynamic. There are many methods described here for keeping a secure platform free of outside threats. However, due to the structure of the network, a hostile node assault is quite likely. That's what causes packet loss. There are a variety of methods that have been recommended by different specialists. The purpose of this project is to use a blacklist and route addresses to locate malicious nodes. HOP and SN are employed from prior strategies in this section. When we talk about route addresses, we're talking about both the route and the node. List of malicious routes that have been examined. There will be a benefit in identifying attacker nodes more quickly [8].

Using mobile ad hoc networks, often called MANETs, has been suggested to allow dynamic situations without infrastructure requirements. Each node in the network serves as a host and a router, delivering data to the other nodes. MANETs, on the other hand, maybe built quickly and inexpensively, in contrast to the time and money necessary to develop wired or wireless infrastructure networks. The MANET is becoming more vulnerable to possible attacks. A "wormhole attack" describes a scenario in which two or more attacker nodes tunnel network traffic from one point to another. On mobile ad hoc networks, wormhole attacks are possible. When two hostile or attacking nodes converge and construct tunnels, it is difficult to determine which nodes did so. An alternate path to the targeted node was discovered using the suggested technique. It is because an invading force could choose the route of least resistance. The secure route discovery protocol is constructed with the assistance of NS2 and a modification of the AODV routing protocol [9].

This research focuses primarily on the performance of MANETs with high resilience to network attacks, such as Grey Hole Attackers and Black Hole Attackers. The other purpose is to fight network attack growth. If the chosen cluster node [2] in a clustered network [3] becomes a malevolent or self-serving node, then the clustered network's [3] data transmission performance will be impaired. Due to the need to protect the cluster head, this action is required. Nodes are picked in this scenario based on their behavior-based trust value and QoS trust metric values. It guarantees that the network is highly resistant to internal and external attackers (compromised nodes) (other nodes). This study helps a technique of clustering based on trust. Malicious nodes are found by evaluating the trustworthiness of every mobile device connected to the network and identifying those with the lowest trustworthiness ratings. The expected degree of trust is considered when adding nodes to the friend list. The members of our group in whom we have the most confidence will assume leadership. The nodes on the buddy list with the lowest levels of trust are eliminated because they are deemed

malicious. The algorithm consists of the following steps: (1) Issue a challenge to neighbors, (2) rate your pals, (3) provide and receive contacts, and (10) rely on the connections.

There are no infrastructure requirements for the Vehicular Adhoc Network (VANET). In a topology that is continually changing, VANET is able to transmit safety data in a time-bound way. VANET's wireless mode makes it easier to break into the system through protocol control messages. As a result, VANET protocol communications must be sent securely. The Secure Optimized Link State Routing (S-OLSR) protocol for VANET was created after a variety of cryptographic techniques were evaluated. ECC uses the features of the elliptic curve to generate encryption keys, while RSA uses the factorization of prime numbers. The end-to-end latency of S-OLSR and ECC was not substantially different, according to the data [11].

In the event of emergencies, natural catastrophes, or other situations in which a radio network is not available, mobile ad hoc networks (MANETs) are an ideal solution since they lack infrastructure and are self-organizing and quick to construct. As a result of MANET'S dynamic topology and constantly changing structures, security may be the most vulnerable point. This leaves it vulnerable to attacks like eavesdropping, routing, and programme modification. When it comes to quality of service, MANET lags far behind because of security problems (QoS). As a result, the most effective method for securing MANET is intrusion monitoring, which entails modifying the system to find other vulnerabilities. In order to provide different degrees of security against unauthorized access, detection of intrusions is a vital component. Failure of a cellular node may impact the cellular node itself and its ability to forward packets, which is defined by the system's overall lifespan. A routing protocol was devised to enhance the number of MANETs accessible for navigation, which led to the consistent and efficient selection of this multi-path. This kind of network is challenging to deliver safe and energy-efficient routing since its topology is constantly changing, and it has a limited number of resources to work. The cat slap single-player algorithm (C-SSA) is used to identify the best forwarding leaps in MANETs to address energy efficiency and security concerns. In the first phase of the process, the fuzzy clustering algorithm is triggered, and the cluster heads (CHs) are selected based on the persons with the highest overall value of indirect, direct, and recent trust.

Additionally, we identified nodes with a trust threshold value. Even the CHs are engaged in multi-hop routing, and the optimal path is determined by considering latency, throughput, and connectivity along this path. The hybrid protocol under examination determines the optimum pathways based on the criteria mentioned above. As a result of implementing the suggested technology, it was feasible to minimize energy consumption to a minimum of 0.11mJ, notice a minimal delay of 0.05ms, and achieve a maximum throughput of 0.74 bps. This strategy was compared to prior methods in the presence and absence of an attack that selectively discarded packets [12]. The outcomes were favorable.

An ad hoc network, also known as a mobile ad hoc network or MANET, is a collection of nodes capable of interacting in an infrastructure-free environment. Individual nodes in these networks are increasingly dependent on one another to perform the network's essential activities. Because there are insufficient resources, it is acceptable for nodes to misbehave to protect what they have. It makes it more challenging to implement secure routing. A technique that can prevent malicious behavior and preserve network synergy is necessary to ensure risk-free routing. Each node in the network adopts a partly distributed dynamic model in order to enhance network security, according to the suggested method. As a precautionary step to maintain safe routing, additional information about network misbehaviour is transmitted to nodes during route building. In the real world, a node may engage in many forms of misbehaviour at various points in time. To cope with nodes that demonstrate different levels of disobedience, it employs a dynamic decision-making method. The model's ability to cope with errant nodes has been shown via simulations [13].

A network mode known as mobile ad hoc networks (MANET) does not rely on a central network infrastructure or access point. MANET's rapid and adaptable networking capabilities allow it to be

used in a broad range of contexts. However, the network's constantly shifting architecture and open communication channels provide security risks. On the basis of these qualities, this paper developed an active routing authentication system (AAS). According to this research, AAS was shown to be successful against attacks such as selective forwarding, fake routing, byzantine, and route spoofing utilizing the BAN logic, even with hostile nodes mixing in the MANET. Tests have shown a 33.9 percent improvement in packet delivery rate, with an average gain of 18.4 percent in networks with malicious nodes. The AAS may be used with several active routing protocols. While the AAS maintains an average connection rate of 1.6 times the collusion attack prevention-OLSR (Cap-OLSR) and 79.2 percent of the network performance in simulated studies with malicious nodes [14], it is also a resilient protocol.

AODV, a widely used routing system for mobile ad hoc networks (MANETs), is susceptible to a blackhole attack despite its widespread adoption. In order to fix the security flaws in the original AODV protocol and prevent the blackhole attack, Lu and colleagues created the SAODV MANET routing protocol. In particular, a malicious node cannot use the SAODV protocol to launch a blackhole attack during the routing process. Blackhole attacks, in which two nodes work together, cannot be thwarted by this defense. So this study presents BP-AODV, a safe MANET routing protocol, to solve the security flaws in SAODV and the original AODV protocols. Aside from that, the BP-AODV can defend against a cooperative blackhole assault launched during routing and a blackhole attack that may occur during the forwarding process. The AODV protocol was extended, and the chaotic map properties were used to create the BP-AODV. Research shows that BP-AODV is more secure than SAODV. It can defend against a rogue node or a group of malicious nodes carrying out blackhole attacks throughout the routing process. The findings also show that the BP-AODV is well-suited to fending off the blackhole assault during forwarding [15].

Finding Black Hole attacks in ad hoc networks (VANETs) and connected and autonomous cars are one of the most challenging and essential routing security concerns (ACVs). Cyber-physical paths may be hacked by malicious vehicles or nodes, converting a safe route into a less secure and dependable. Hostile nodes intentionally skip neighboring nodes and discard data packets that could include emergency alert signals instead of passing them on. This study devises an IDBA (intelligent black hole attack detection technique) to identify ACV-specific black hole attacks better. Hop Count, Destination Sequence Number, Packet Delivery Ratio (PDR), and End-to-End Delay are just a few of the crucial factors in this study (E2E). IDBA was evaluated against AODV using the Black Hole (BAODV), Intrusion Detection System (IdsAODV), and EAODV algorithms. PDR, E2E, routing overhead, packet loss rate, and throughput is much better with our IDBA than with current techniques [16].

Due to the lack of base stations and access points, mobile ad hoc networks (MANET) are vulnerable to jamming assaults, the most prevalent kind. Because IP-based routing is often used in ad hoc networks, it is essential to keep safe and secure communication between nodes. The goal of this research is to examine the performance of the MANET when IPsec is used and determine if IPsec is successful in protecting the MANET from jamming attacks. Mobile nodes with and without IPsec may be compared using the Riverbed Modeler Academic Edition simulator. It simulates Ad hoc On-Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), and Temporarily Ordered Routing Algorithm (TORA) protocols (TORA). Simulation findings show that the AODV routing protocol causes the most significant percentage increase in latency and retransmission attempts under typical operations. AODV's throughput is the greatest while it is under assault, however. OLSR has the most significant number of delays and retransmission attempts [17].

For a variety of uses, such as military, entertainment, commerce, and emergency services, MANETs have become more important. Nodes in the MANET may be exposed to malevolent actors because of the network's openness and decentralisation. One of the most significant characteristics of MANET is anonymity. The anonymity of the MANET has been the subject of a lot of study in the past several years. In order to protect the MANET's anonymity, many routing protocols, like as

GSPR, AO2P, ALARM, PRISM, and ASR, have been developed. In addition to their high costs and the inability to provide total anonymity for all three parties involved, each of these methods has certain drawbacks. The ALERT protocol was developed to address the aforementioned difficulties and is notable for its cheap cost and preservation of source, destination, and route anonymity. In order to avoid DoS and Man in the Middle attacks on ALERT utilising Hash function and SHA-1 algorithm [18], this study proposes to use an approach that uses the ALERT protocol but does not provide security against active assaults.

3. Optimization of the Secure Channel for Application in MANET

In addition, the problem, as well as some potential solutions, are discussed in this section. Altering the regular serves as the cluster leader is one of the best ways to extend the life of a network. The function that determines the cluster head is denoted by the notation T(CH), and it is the function that always gives the cluster head. A collection of separate entities is referred to as Instance G.

$$\forall g \subset G \qquad \text{(Eq. 1)}$$

In every given cluster, N is the total number of nodes, and k is the number of rounds.

$$\varnothing(g) \neq NULL \qquad \text{(Eq. 2)}$$

In order to prove the lemma that came before it, we will now demonstrate that there is a cluster g in the whole network that satisfies the following condition: (Eq. 2) the number of non-dead or active nodes is not zero.

$$\forall n \subset N \qquad \text{(Eq. 3)}$$

In addition, the selected node, denoted by the symbol n in Equation 3, and the node that will be picked at random to serve as the new cluster head are denoted by the symbol n'.

$$\forall n(t) \subset N' \qquad \text{(Eq. 4)}$$

Eleventh-order polynomial,

$$N \notin N' \; and \; N' \notin N \quad \text{(Eq. 5)}$$

Because, (Eq. 4) thus the newly picked cluster head may avoid being comparable to the previous one.

$$1 - R(k)[\mathrm{k}.\mathrm{mod}\frac{1}{R(k)}] \qquad \text{(Eq. 6)}$$

If R(k) stands for the percentage of cluster heads within N that are still accessible, then (Eq. 5) reflects the remaining percentage of cluster heads inside N that are still available. As a direct consequence of this, the cluster dead decision function may be written down as follows:

$$T(CH) = \frac{R(k)}{1 - R(k)[\mathrm{k}.\mathrm{mod}\frac{1}{R(k)}]} \qquad \text{(Eq. 7)}$$

The energy usage is likewise uniformly distributed since the Eq. 8 clearly stands for not repeating cluster heads in later periods.

$$CH = \prod_{\mathrm{Re}s(N\_Egy(n))}^{Max(N\_Egy(n))} n \oplus [n \subset N \notin D] \qquad \text{(Eq. 8)}$$

Further, in the next section, the proposed algorithm is furnished.

4. Novel route-optimized cluster-based algorithm

The proposed algorithm is furnished here:

Step - 1. Initialize MANET nodes i=0 to n as follows:

a. If (nodes are in range of Ln)
   i. So (apply the SHA-3 algorithm)
   ii. //It uses SHA3 to build a hash.
   iii. A united identification

b. else
   i. isn't Ln, but

c. if
   i. a halt
   ii. Rep for I = 0 to n.
   iii. Follow the reasoning to verify j=j+1.
   iv. An(i, j) share a
   v. Other Ln id
      1. if (nodes) accepts
      2. an identifier accepted by all
      3. the data to L(n) as the node provides trustworthy information

d. else
   i. "Node" means "malicious."

e. if
   i. Now SHA-3 the source node (S)
   ii. Send RREQ packets from source.
   iii. So, if (Source and Destination nodes)
   iv. if both nodes and the ln are controlled,

1. RREQ Forward Destination
2. Node (D)
3. To verify the legitimacy of the
4. The authenticity and integrity of the tree's root

f. else
1. RREQ A future (i,j)

g. else

h. Stop

The subsequent portion of this paper analyses the acquired findings in light of the method presented.

5. Results and Discussions

In the next portion of the paper, the acquired findings are examined side by side using a comparison approach [Table 1]. The simulation is run a total of one hundred times via iterations. On the other hand, the findings are shown for a sample size of 25 iterations.

Table 1: Secure Routing Simulation Analysis

Number of Nodes	Randomly Selected Channels	Duration of Transmission (ns)	TEEN – Identity Leaks	SEP – Identity Leaks	Proposed Method – Identity Leaks
166	3	0.6213	9	6	4
103	5	0.1985	8	6	3
393	4	0.8709	8	7	5
27	5	0.3065	10	6	5
443	3	0.6097	9	6	5
500	3	0.8956	10	6	3
497	3	0.8545	9	7	3
205	4	0.3181	10	7	5
374	3	0.6723	10	6	4
14	3	0.4324	9	7	5
164	3	0.4204	9	7	4
330	5	0.843	10	7	5
53	3	0.882	8	6	5
161	3	0.769	9	7	4
368	5	0.8698	10	6	3

494	4	0.5342	10	7	5
488	4	0.8324	9	7	4
222	3	0.6706	9	6	4
311	5	0.9858	9	6	3
491	4	0.6821	8	7	3
17	4	0.1846	10	7	4
440	4	0.9747	9	7	5
108	5	0.4143	9	6	4
281	3	0.6073	9	7	3

The improved results are visualized graphically here [Fig – 1 to 6].

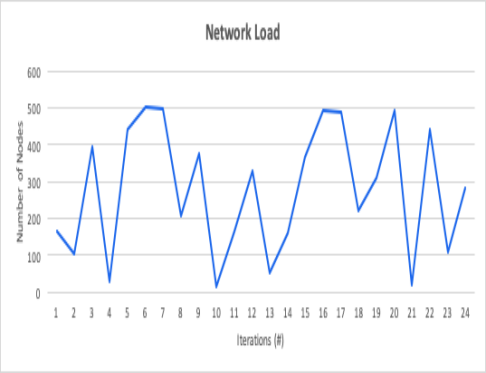

Figure 1: Network Load Analysis

Anomalies, such as security and operational problems, can be detected through NTA, a technique for monitoring network availability and activity. Use cases for NTA are as follows: Keeping a running log of all network activity, both current and historical. Anti-malware software that can identify threats like ransomware.

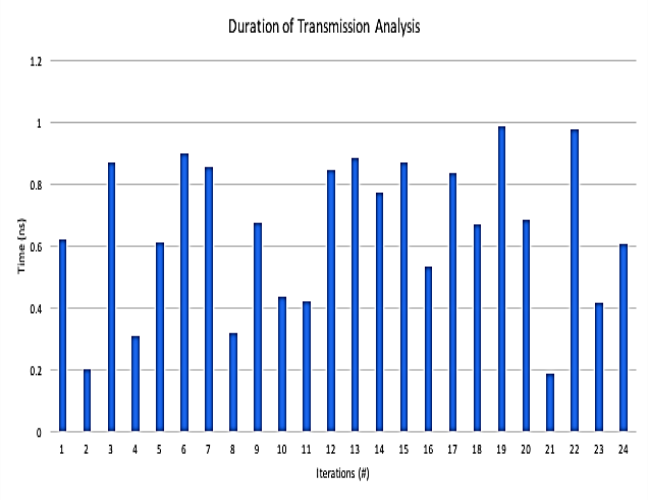

Figure 2: Duration Analysis

It is a model used in WSN or MANET to analyse large projects and determine how changes in input variables affect the target variable. Simulated results are used to predict how a decision would change if we changed a set of input variables in a certain range.

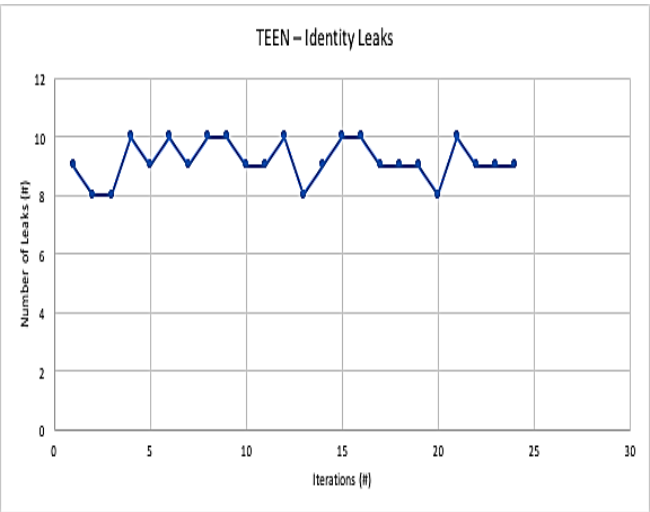

Figure 3: Leak Analysis for TEEN

Wireless ad-hoc networks may offer benefits over wireless managed networks in some applications where it is impossible to rely on central nodes. The theoretical and actual limitations have been established to the total network capacity. Since they need very little preparation and can be set up in minutes, ad hoc networks are well suited for usage in crisis circumstances such as those brought on by natural disasters or by armed conflicts. Dynamic and adaptive routing protocols allow for the formation of ad hoc networks in a concise amount of time. Ad hoc wireless networks may be further classified into several categories according to the tasks used.

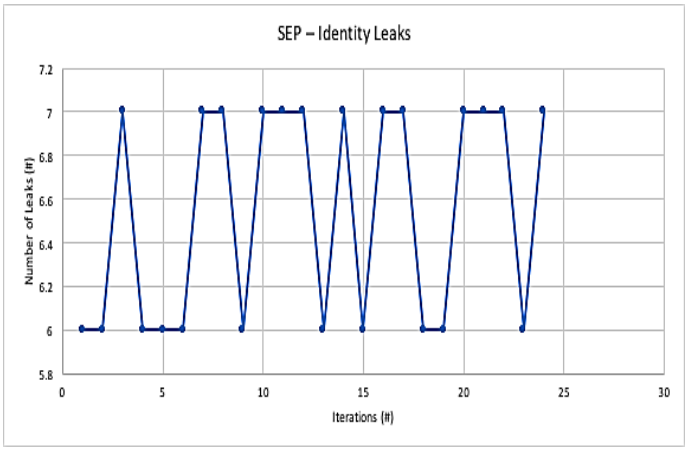

Figure 4: Leak Analysis for SEP

However, ad-hoc wireless networks may provide benefits over wireless managed networks in some applications. The central nodes cannot be depended on even though it has been shown that the

total network capacity is subject to theoretical and practical restrictions. Because they require minimal preparation and can be set up in minutes, ad hoc networks are useful for emergency scenarios such as natural disasters or military conflicts. It makes them perfect for disaster relief and military operations because they can be set up in such a short amount of time. Ad hoc networks may be created in a concise amount of time thanks to routing algorithms that are both dynamic and flexible. Other categories may be created for ad hoc wireless networks, depending on the applications that utilize them.

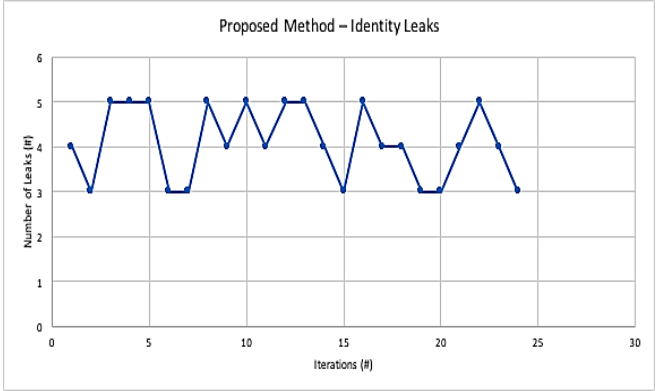

Figure 5: Leak Analysis for Proposed Method

The capacity of the whole network is restricted due to a combination of theoretical and practical considerations. On the other hand, ad-hoc wireless networks may perform better than wireless managed networks in some applications with no central nodes. It is because a central authority does not maintain ad-hoc networks. Because they do not need much preparation and can be put up in just a few minutes, ad hoc networks are helpful for use in crisis circumstances such as those brought on by natural catastrophes or armed conflicts. Because of this, they are suitable for use in military activities and disaster assistance. Protocols that are both dynamic and adaptable allow the creation of ad hoc networks simple and possible in a short period. They are further subdivided into categories determined by the purposes for which they are utilized.

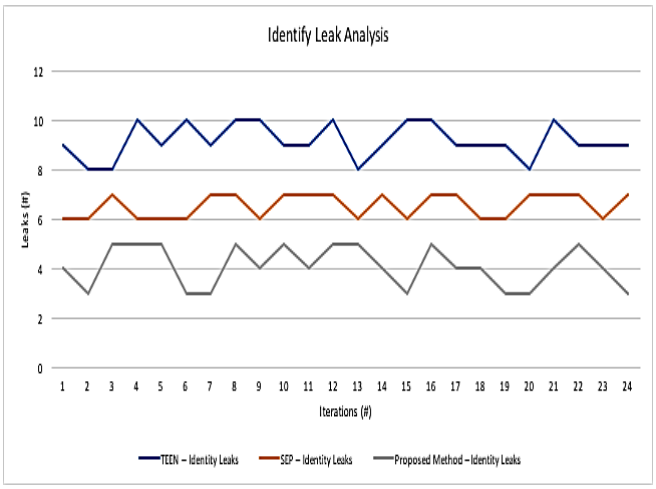

Figure 6: Comparative Analysis - Leak Analysis

Further, the research conclusion is presented in the next section.

6. Conclusion

This paper develops and designs a novel cluster-based routing technique to boost the cluster head selection time and the energy efficiency of the routing algorithms used in sensor networks. The research demonstrates that improved results are achieved compared to the earlier methods. During the inquiry, the work demonstrates the classifications of the routing algorithms for Sensor Networks, along with their essential rejection criteria for each specific network. The effectiveness of TEEN, SEP, and EAMMH concerning the specified systems is investigated in this research. It has been proved that the algorithm has a higher energy economy and consistency when applied to a tactical Sensor Network. This work will, in the end, result in a one-of-a-kind algorithm with a time savings of around fifty percent, an increase of fifty percent in power awareness, and a supplied technique for assessing the energy efficiency of any given algorithm that will be used in following updates.

References

[1] Y. K. Alapati and S. Ravichandran, "Efficient Route Identification Method for Secure Packets Transfer in MANET," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 467-471.

[2] N. Yadav and U. Chug, "Secure Routing in MANET:A Review," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 375-379.

[3] V. S. Bhargavi, M. Seetha and S. Viswanadharaju, "A trust based secure routing scheme for MANETS," 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, India, 2016, pp. 565-570.

[4] S. Yadav, M. C. Trivedi, V. K. Singh and M. L. Kolhe, "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme," 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), Mathura, India, 2017, pp. 1-4.

[5] S. R. Deshmukh and P. N. Chatur, "Secure routing to avoid black hole affected routes in MANET," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 2016, pp. 1-4.

[6] S. Sharma, "A secure reputation based architecture for MANET routing," 2017 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 2017, pp. 106-110.

[7] S. R. Deshmukh, P. N. Chatur and N. B. Bhople, "AODV-based secure routing against blackhole attack in MANET," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2016, pp. 1960-1964.

[8] K. Singh and S. Sharma, "A new technique for AODV based secure routing with detection black hole in MANET," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 1528-1534.

[9] C. Gupta and P. Pathak, "Movement based or neighbor based tehnique for preventing wormhole attack in MANET," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 2016, pp. 1-5.

[10] S. B. Kulkarni and B. N. Yuvaraju, "Rating and friend sharing algorithm of trust based clustered routing algorithm in MANETS," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 843-846.

[11] P. Yellanki and M. V. S. P. Narasimham, "Secure Routing Protocol for VANETS using ECC," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-5.
[12] N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," in IEEE Access, vol. 9, pp. 120996-121005, 2021.
[13] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," in Journal of Communications and Networks, vol. 18, no. 6, pp. 938-947, Dec. 2016.
[14] J. Tu, D. Tian and Y. Wang, "An Active-Routing Authentication Scheme in MANET," in IEEE Access, vol. 9, pp. 34276-34286, 2021.
[15] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019.
[16] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles," in IEEE Access, vol. 8, pp. 199618-199628, 2020.
[17] F. Hamadah, M. A. Rahman and T. W. Au, "Impact of IPSec on MANET," 2016 International Symposium on Computer, Consumer and Control (IS3C), Xi'an, China, 2016, pp. 408-411.
[18] P. Patil, N. Marathe and V. Jethani, "Preventing DOS & MITM Attacks in “anonymous location based efficient routing protocol” in MANET," 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, India, 2016, pp. 16-20.