International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

Secure and Energy Efficient Routing Protocols for MANET using BAT Optimization

Dr.K.Muthumayil[1] Dr.M.Buvana[2] and Dr.T.Jayasankar[3]

[1]Professor , Dept.of IT , PSNA College of Engineeringngineering and Technology, Dindigul,Tamilnadu
[2]Associate Professor, Dept of CSE , PSNA College of Engineering and Technology, Dindigul,Tamilnadu
[3]Assistant Professor, Dept of ECE , University College of Engineering,BIT Campus, Tiruchirapalli,Tamilnadu
[1]muthumayil@psnacet.edu.in [2]buvana@psnacet.edu.in [3]jayasankar27681@gmail.com

Abstract

Recent advances in mobile ad-hoc mobile dynamics improve network speed and stability. The nodes in the ad-hoc hierarchical network move in nature. Due to increased network subscribers, network traffic has grown to a higher level which, in turn, preserves the energy. The route optimization method in the mobile ad hoc network uses more resources and efficiency and connectivity depends on the drainage of electricity. In addition, the network is often affected by dangerous attacks, such as denial of service, black hole attack. This paper focuses primarily on preventing these attacks by using the complex ad hoc mobile network to improve demand protocol and BAT and on reducing the rate of energy drainage. The velocity and fitness value of the nodes are calculated for this. The empirical simulation findings of the Bat BAT algorithm indicate that the transmission is energy efficient and secure. The efficiency metrics of overhead and execution time were decreased and BAT optimization in a complex mobile ad hoc network scenario improved steadily as a result.

Keyword: BAT optimization, dynamic mobile ad-hoc network, routing and black hole detection.

1 Introduction

The recent developments in network technologies make the wireless network as an important role in Systems of data exchange. The Internet of versatility is obviously well suited for accessing resources on the Internet at any time or anywhere in our daily lives. Many new smartphone apps come every day, allowing us to comfort our day-to-day needs, such as booking seats on buses, trains or airports, exploring new places etc. In addition, further devices in the wireless network ecosystem can cause more security problems in the network and can be managed efficiently to ensure safe data transfer across the wireless network. In MANET, the implementation of security schemes has several problems, owing to secure wireless connections, power limitations, daunting condition of weak physical safety of nodes, node mobility, dynamically changes in topologies, etc.[1]. The lack of fixed infrastructure would further exacerbate the issue of developing safe MANET environmental routing systems in which free moving node links with their neighbours. Any node can at all times join or leave the network domain without warning, and in most situations is difficult to provide a clear image of the membership of the network. For MANET, which is categorized as a proactive and a reactive protocol in two categories[2], several routing protocols are suggested.

Each mobile node has a routing table with a list of all possible destinations in constructive protocols. These tables are updated regularly across the network by transmitting routing information. The benefit of keeping the routing table is that nodes will connect with each other immediately if routes are present in a table. The most important influence during routing is the mobility of nodes within the ad hoc network. Generally, nodes at MANET will travel in either direction independently and

dynamically alter their routes. And every MANET node is called a router for finding and maintaining new routes. Each node has to discover the path to the destination. Moreover, multi-hop strategy is applied via certain intermediate nodes if the node needs to communicate with another node outside its broadcasting radius. Even in uncertain times, the topology of this kind of networks also changes[3]. To increase the performance of MANET, there would be some limitations to overcome: The features of the wireless connection differ with time. Multiple factors limit the reliability of wireless node transmissions. Some features such as track failure, package loss, and incorrect inference impair the stability of MANET nodes. Wireless Internet MANET transmission is restricted only. Compared to wired networks, the frequency cap for radio data speeds is lower. Bandwidth consumption will then be low if overhead is kept less. A routing protocol is used to discover the best routes between the nodes in order to provide a completely random, infrastructure-less networking and effective end-to-end connectivity with the networks of nodes. Therefore, the primary difficulty is to find a suitable and reliable path from one node to another and to guarantee the packets are sent correctly and promptly[5]. The Routing Protocols intended for wired networks cannot be used for MANETs because the complex structure of the mobile nodes makes routing in MANETs non-trivial. A minimal overhead and bandwidth utilization should be performed on the route construction. Until MANETs are deployed successfully, security problems must be resolved. Cryptographic methods are usually used for secure wired and wireless communications. The issue of Black hole attack is that we need a way to send packets successfully to MANETs. This problem is created by the malicious node or intruder node that is the usual node, which is the shortest path the packet has to send to the destination node. Based on the false reaction from the malicious node, a blackhole attack is detected. Malicious node detected is put in the blacklist and is sent to the network's nodes [6].

The approach to using conventional wired network safety solutions is not appropriate for MANET security. Each shared-key authentication system's biggest challenge is making the public key for each user accessible to others in a way that verifies its authenticity. Common security solutions for public key management (PKI) are introduced through the holding of public key certificates from any participating entity and through the provision of the online Certification Authority (CA) a trusted third party(TTP) maintains public key certificates. MANETs do not allow trusted authorities or centralized servers to access their services online [7]. Implementing public and certificate administration is more difficult due to the issue of key exchanges and the session processing, lack of infrastructure and unified facilities, constant node mobility, insecurity of wireless connection, potential network partitions, and on-the-fly setup of all network services. Traditional security services requiring confidential on-line authority or archives of certificates are not suitable to secure MANETs. One of the successful ways to secure MANET is to use public key encryption and certificates.

2 Literature Review

Manish Bhardwaj[8] introduced a protocol to respond to the problem of decreased electricity supply by reducing energy efficiency. The first was a wireless network charging solution and the second was to provide energy-saving routing protocols to enhance the networks. Two options were presented. They also attempt to minimize overheads, stability and speed convergence.

Senthilnathan & Kalaiarasan [9] suggested a robust energy-efficient routing with the use of MANET tracking agents. Monitoring agents quantify the details about links between the nodes. In this job. Connection node stability measures include the period and the accurate period of linkage. The relation packet error rate and signal strength are also calculated in this work. This decreases energy demand and increases the distribution ratio of packets.

The Binary Particle Swarm Optimization (BPSO) algorithm has been proposed by Shahram Jamali et al.[10]. This technology incorporates the absorption of energy as part of the TORA protocol. This suggested protocol measures the node energy level before and after node routing. It also takes into

account roads and their length for the route to calculate the energy level required to calculate the route. The tests carried out show that the BPSO protocol suggested works better than TORA to ensure that nodes are kept alive, throughput, scalable and network life.

Salinkhe & Patil [11] presented MANET with an effective delay among nodes for an anonymous, stable routing. The goal of this paper is to ensure secured communication between nodes by integrating effective authenticated anonymous safe routing and to increase the efficiency of packet delays.

3 Proposed Methodology

The suggested workflow approach is to estimate the node's fitness and speed. By using the BAT optimization technology. The explanation for this implementation is that the original node x and the next node Y are found at the highest speed. Each node sends packets into the network initially if node I = 0, i>n finds the best value location. It automatically updates the best P value if pb is 1 then it calculates node speed and transfers the node as I increase. This process continues until the target node.

3.1 Route discovery on demand distance vector

The route as the cumulative function is an essential feature that differs from the ad hoc on demand protocol that allows complex mobile ad hoc on demand protocol. If the initial node has no entry in its final node, it will transmit the message to its neighbor. Then, the next node answers to the final node by sending a path request with a route response code. Whenever a path request is made, if a neighboring node has an entry into the final node, the route response knowledge answers. Otherwise, the path request message is transmitted. The router changes its sequence number every time a path request is sent. If there is the same sequence number on the incoming packets, the same information will be discarded. The next node connects the address along with the post. During this phase. The middle node marks the reverse path. Energy saving functionality is also available for dynamic mobile on call. If the energy of a node is too poor, the node can't be more involved in road exploration. The roads are built in this way.

3.2 Route maintenance on demand distance vector

Every node must check the status of the links during the routing process and also keeps the latest update inside the tables. With the help of path error signals the route conservation process remains proficient. This message was only produced if one of the nodes split. The routing table will be changed with the response to this post. The broken nodes entry will be cancelled at the same time. The management of the route in dynamic mobile ad hoc on demand protocol is broken with the relation of Node 6 and Node 7 and Node 6 with the node 7 information. The time stamp for a node expired at that time in the route entry and the route entry should be invalid. Node 6 then transmits the node 1 error message. The low mobility is not the product of the complex MANET on demand protocol. It is really good because there is a path of traffic after any network.

3.3 BAT algorithm

If the characteristic echolocation of the micro bat is idealized, various algorithms inspired by bat are created. The idealized laws are these:

1. A position echo technique is used to feel the distance bat. They describe both the context and food obstacles in certain respects

2. In this context vi is to be regarded as the speed while xi is to be understood as the location of the random flying bat within the restricted minimum frequency (fmin). You adjust the wavelengths of K when looking for its prey, with the loudness of A0. Usually, the bat change its wavelength and pulse emission rate r[[[0, 1] to the target, depending on how near it is.

3. Since the loudness varies from broad A0 to minimal constant value of Amin, it is generally assumed that loudness differed from wide A0. The following calculations are used in order to be simple. The wavelength of the frequency f, which is [k min, k max], is the [fmin, fmax, fmin] range. In cases where the issue lies, recommend using any wavelength because it is easy to apply [17, 18]. The frequency can also be altered simultaneously when the wavelength can be fixed. This is because k and f remain connected and k f remains stable. There must be certain guidelines to update the location of xi and speed vi.

The following equations indicate the solutions xti as well as speeds vti in phase t. while in Eq. 6 [0, 1], the random vector computed from the uniform distribution is indicated and x*, after all possible solutions were compared between all n bat.

$$f_i = f_{min} + (f_{max} - f_{min})\beta$$

4 Simulation Result

The proposed BAT dynamic routing protocol performance assessment is analyzed by the current protocols with respect to identification of blackhole. The distinction between the BAT protocol and the other protocols for blackhole identification. Comparing the current protocols, it may be inferred that the proposed Dynamic BAT method routing protocol is 20-40% blackhole detection.

4.1 Performance Evaluation

The performance of the proposed protocol is compared with the existing protocols in terms Packet delivery ratio (PDR), End-End Delay, Energy Utilization and Blackhole Detection.

End- End Delay

The pause of the protocol suggested for other protocols can be seen in Figure 1. We may infer that there is a delay of 10ms to 50ms less than the present protocols in the proposed approach.

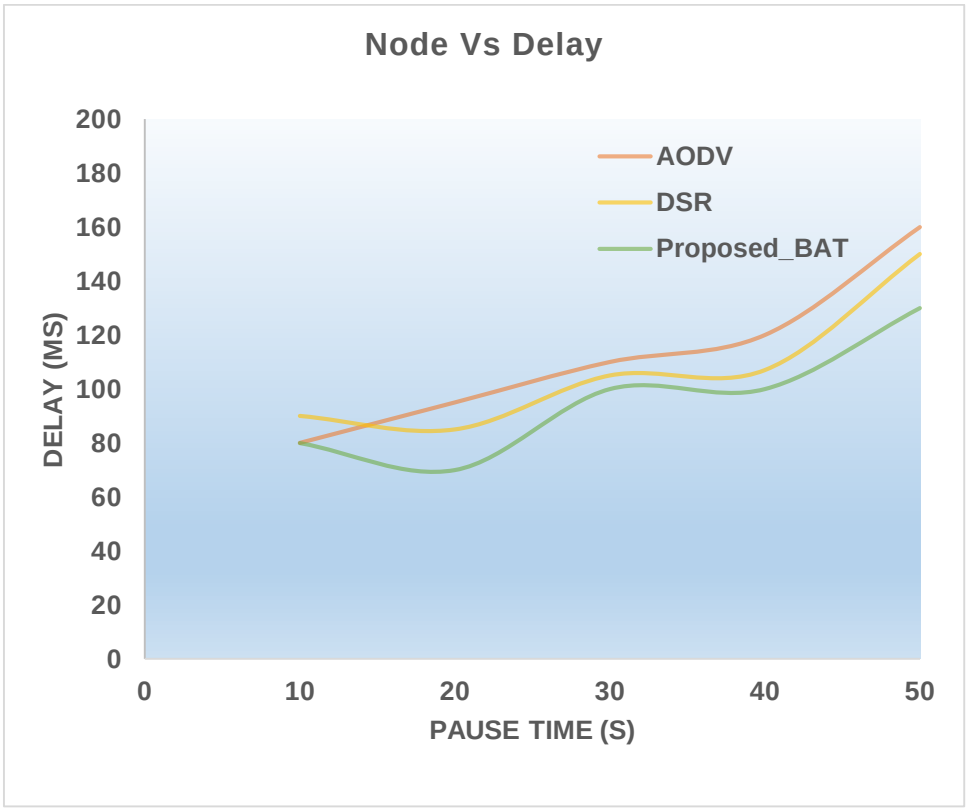

Figure 1. Comparisons of End- End Delay

Packet Delivery Ratio

Figure 2 provides a comparison of the protocol proposed to other protocols for the packet delivery ratio. And if the number of nodes increases, the BAT packet distribution ratio is comparatively high. The package distribution ratio is greater than the current protocols of the solution proposed.

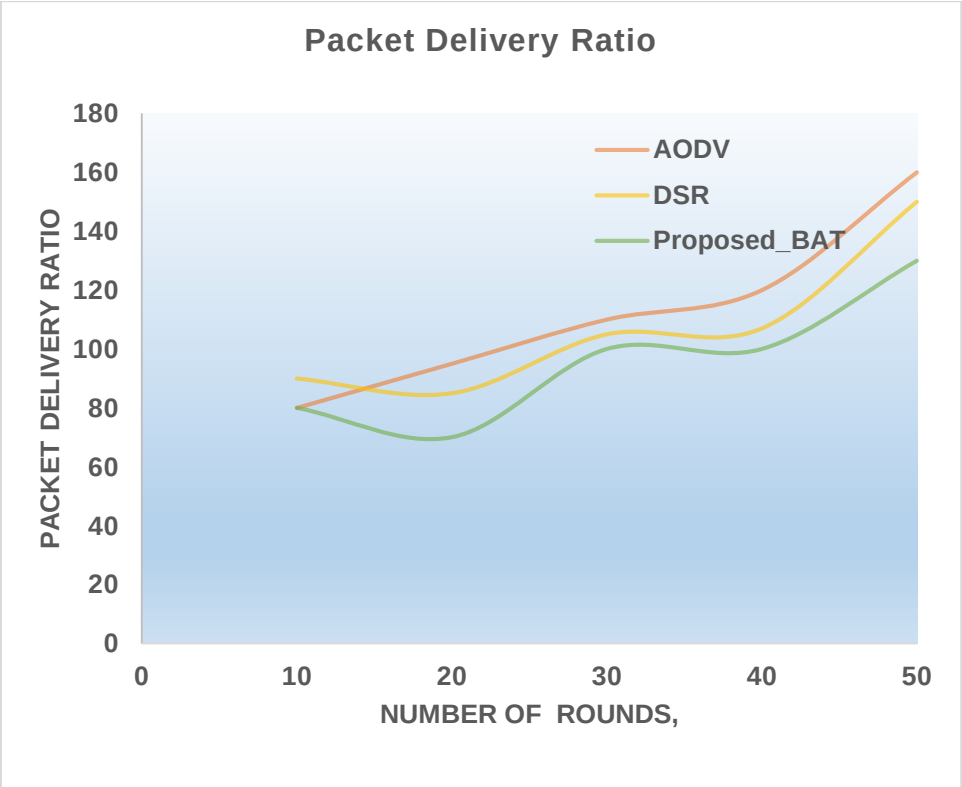

Figure 2. Comparisons of Packet Delivery Ratio

Energy Utilization

Figure 3 illustrates the relation with other protocols of energy consumption of the proposed protocol. Compared to other existing protocols, energy consumption is relatively limited. In comparison with the current protocols, it can be inferred that the new solution saves less space. The energy consumption of nodes is greater than current protocols but not AODV when nodes are increased. The relation of DSR-AODV energy consumption.

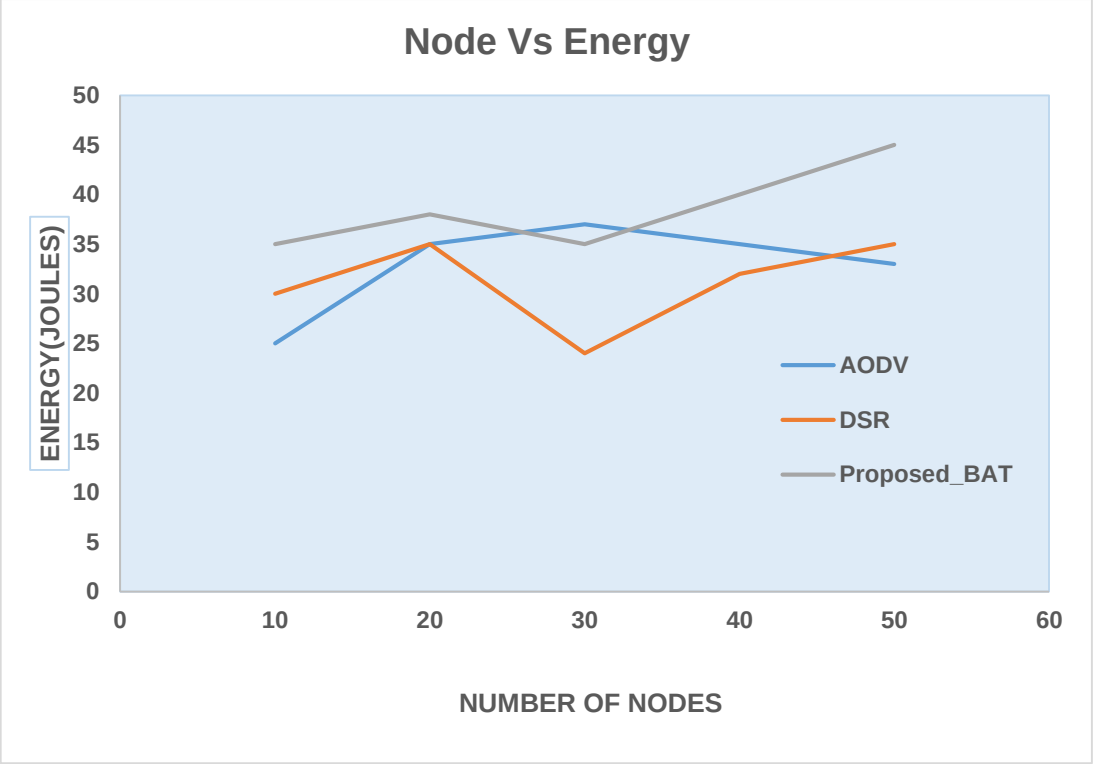

Figure 3. Comparisons of Energy Utilization

Blackhole Detection

Black hole attack is kind of DoS attack where the malicious node advertise itself as a fresh node by sending fake information. After that, misuse the data or drop the data packet instead of routing them to the destination node by this way, the information should not reach the destination node by this kind of attack. Normally, black hole attack is carried out by the node inside the network. Figure 4 displays the comparison between the blackhole detection protocol proposed and the other protocols.

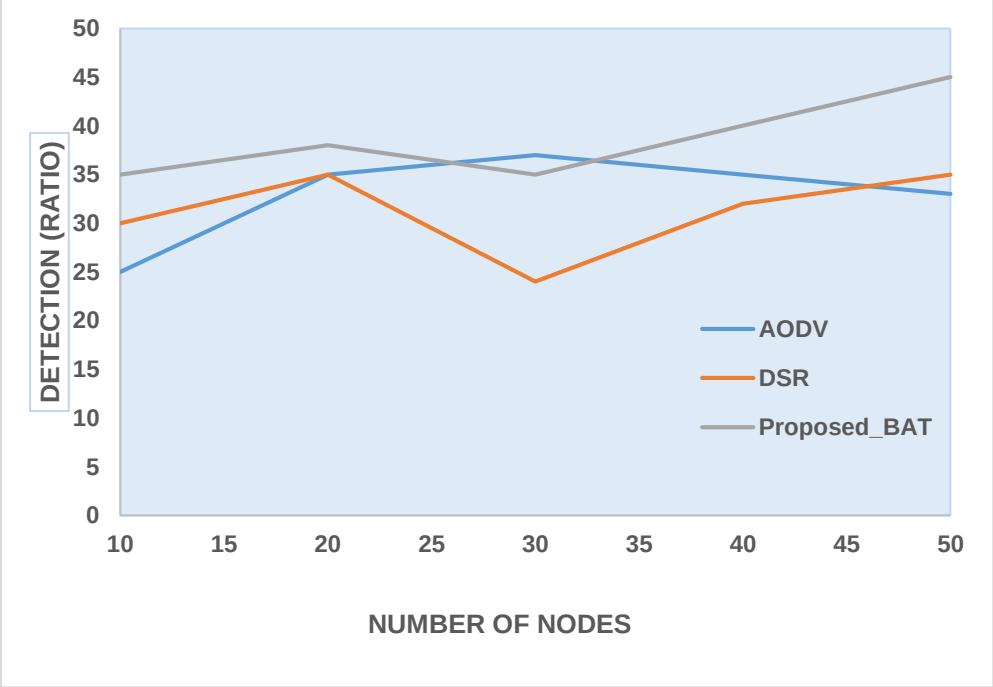

Figure 4. Comparisons of Blackhole Detection

The suggested solution has been improved by 20%-40% as comparing with current protocols in blackhole identification.

5 Conclusion

An enhanced DSR routing protocol version is suggested. The bee food quest theory is used to accomplish this change. The mobile dynamic ad-hoc protocol network selects routes by using secure routing techniques. This helps to find the shortest route to the destination and increases the secure delivery of the packet in the dynamic network. The simulation results show that in comparison to the existing AODV, DSR routing protocol, the packet delivery ratio and end-to-end delay in dynamic mobile ad-hoc network with BAT optimisation are further improved. In comparison with current protocols the proposed approach has risen by 20% - 40% in blackhole detection.

Reference

[1]. Pandey S, Yadav RS. Study of Location Based Energy Efficient AODV Routing Protocols In MANET. International Journal of Engineering Inventions. 2013;3(2):1-5.
[2]. Jain HR, Sharma SK. Improved energy efficient secure multipath AODV routing protocol for MANET. In2014 International Conference on Advances in Engineering & Technology Research (ICAETR-2014) 2014 Aug 1 (pp. 1-9). IEEE.
[3]. Sharma R, Sharma T, Kalia A. A comparative review on routing protocols in MANET. International Journal of Computer Applications. 2016 Jan;133(1):33-8.
[4]. Patel DN, Patel SB, Kothadiya HR, Jethwa PD, Jhaveri RH. A survey of reactive routing protocols in MANET. InInternational Conference on Information Communication and Embedded Systems (ICICES2014) 2014 Feb 27 (pp. 1-6). IEEE.
[5]. Kumar GV, Reddyr YV, Nagendra M. Current research work on routing protocols for MANET: a literature survey. international Journal on computer Science and Engineering. 2010 May;2(3):706-13.

[6]. Singh T, Singh J, Sharma S. Energy efficient secured routing protocol for MANETs. Wireless Networks. 2017 May 1;23(4):1001-9.
[7]. Patil JA, Sidnal N. Survey-secure routing protocols of MANET. International Journal of Applied Information Systems (IJAIS). 2013 Mar;5(4).
[8]. Manish Bhardwaj 2015, 'Enhance Life Time of Mobile Ad-hoc Network Using WiTriCity and Backpressure Technique', Proceedings of the International conference on Recent Trends in Computing, vol. 57, no. 1, pp. 1342-1350.
[9]. Manikandan, T, S.Shitharth, Senthilkumar, C , Sebastinalbina, C & Kamaraj, N 2014, 'Removal of Selective Black Hole Attack in MANET by AODV Protoco', International Journal of Innovative Research in Science, Engineering and Technology, vol. 3, no. 3, pp. 2372-2377.
[10].ShahramJamali, Leila RezaeiSajjad & Jahanbakhsh Gudakahriz 2015, 'An Energy-Efficient Routing Protocol for MANETs: a Particle Swarm Optimization Approach', Journal of Applied Research and Technology, vol. 11, no. 6, pp. 803-812.
[11].Salunkhe, SP & Patil, HD 2016,'Delay Efficient Authenticated Anonymous Secure Routing for MANETs', International Journal of Computer Applications, vol. 148, no. 4