Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3240 – 3252
Received 20 January 2021; Accepted 08 February 2021.

A Review on Secure Multipath Routing Schemes for MANETs

[1]Yarlagadda Sirisha, [2]Pamidi Naga Venkata Siva Kumar, [3]Nagendra Babu Rajaboina

[1]Assistant professor, ECEdepartment, Vijaya institute of technology for women,
yarlagaddasirisha1@gmail.com

[2]Assistant Professor, ECE department, Vijaya institute of technology for women,
sivakumar.pamidi@gmail.com

[3]Assistant Professor, CSE department, Vijaya institute of technology for women,
nagendrarajaboina@gmail.com

Abstract

Study has substantially investigated routing protocols in ad hoc networks. Most state-of-the-art surveys have concentrated on evaluating and classifying the numerous routing structures suggested for MANET depending on the form of network and the application of the protocol. Security dimensions of routing protocols were not provided adequate consideration and most of MANET's routing protocols were not developed with security specifications in mind. However, protection is a concern, taking into account that ad hoc network applications ought to help essential infrastructures (i.e. defense, healthcare, environmental, etc.). And because these infrastructures are highly reliant on the availability of capital, particular emphasis has been put on supporting a stable, robust, and efficient environment, with one of the added features being multipath routing. The need for protection in fragile ad hoc network implementations has driven researchers from the beginning to develop protected multipath routing protocols or to design security enhancements for established protocols. The present state-of-the-art of secure multipath routing protocols in ad hoc networks is studied in this article.

Keywords:MANET, Secure multipath routing, Multipath routing, Security

1.Intruduction

In recent years, the Mobile Ad Hoc Network (MANET) has grown rapidly and promises to be one of the basic infrastructures for promoting environmental intelligence. Ad hoc networks are currently being encouraged to be utilized in a broad variety of environments, such as military, healthcare, and environmental applications, where extremely confidential knowledge is handled.

This suggests that in these mission-critical contexts, data comptonization is inappropriate when they depend on timely and accurate details to deliver their services. There are several threats in an ad hoc network that can undermine the network and its records. Security in vital MANET infrastructures is therefore important and must be handled in order to secure the network and its records. In order to facilitate a secure defense architecture that would be able to cope easily and reliably with disruptive behavior that seeks to undermine the MANET, security should be enabled by fundamental MANET operations. Routing that defines contact paths between sensor nodes and forwards data from a source to a destination node is such an operation. In MANETs, where resources are scarce, the standard practice is to create single-path routing between nodes of the source and destination. Failure of nodes in the path, though, will imply path failure and data loss. In comparison, if routing is corrupted, then the entire ad hoc is at risk. In the sense of critical software, it is considered crucial to develop stability and availability for an application to effectively serve its goals. Approaches have been planned to include several routes to increase the network's availability, resilience, and efficiency. The usage of several routes, however, raises potential security issues when it allows details accessible at multiple sites, providing adversaries more opportunity to hack the details. In critical environments, it is also necessary to defend the network from malicious behavior in order to increase and sustain the network's availability and reliability. Currently, since most of the routing protocols in MANETs have not been developed with security specifications in mind, security problems in multipath routing have not been given adequate consideration. The aim of this research work is to explore safety problems in multipath routing in MANETs. A detailed analysis of stable multipath MANET routing protocols is presented in this article.

2.Literature Review

Veeraiah, N., Krishna, B.T[1] suggests, based on an optimization algorithm, a powerful multipath routing protocol in MANET. The MANET energy and protection crisis is efficiently tackled using the collection and intrusion mitigation techniques of the cluster head (CH), including fuzzy clustering and fuzzy Naive Bayes (fuzzy NB). The multipath routing is then progressed using the Bird Swarm-Whale Optimization Algorithm (BSWOA), which is the incorporation of bird swarm optimization (BSA) into the whale optimization algorithm, based on the routing protocol (WOA).

Borkar, G.M., Mahajan, A.R[2] suggested mesh-based multipath routing method to use the Dolphin Echolocation Algorithm for efficient contact in MANET to discover all feasible safe paths using secure adjacent place confidence verification protocol and better connection optimal path locate. The performance review and numerical results show that improved packet distribution ratios, reduced packet delays, reduced overheads and protection against vulnerabilities and attacks are created by our proposed routing protocol.

A. Taha, M. Uddin, R. Alsaqour, M. Abdelhaq and T. In the Ad Hoc On Demand Multipath Distance Vector (AOMDV) routing protocol, Saba[3] suggested an algorithm that illustrates the unique problem of energy consumption in MANET by applying the Exercise Feature technique to maximise energy consumption. The suggested protocol is named the Multipath Distance Vector with the Exercise Feature Ad Hoc On Demand (FF-AOMDV). In multipath routing, the exercise function is used to find the optimum route from the source to the destination to decrease energy usage. The comparison was measured on the basis of efficiency parameters for energy usage, throughput, packet distribution ratio, end-to-end delay, network lifetime and routing overhead ratio, node speed, packet size and simulation time variations.

H. S. and R. Jain. K. Sharma[4] The suggested solution requires an adaptive strategy in which the energy performance of our proposed scheme is greater. The filtering forwarding scheme slows down the spread of excessive RREQs generated per unit time by a node and prevents Denial of Service attacks with success. This paper envisaged multipath extensions and a security enhancement toward the AODV routing protocol.

The hash function with location update algorithm is proposed in the Ad hoc On-Demand Distance Vector (AODV) routing protocol to boost protection against selfish nodes in Mallikarjuna Anantapur, VenkanagoudaChanabasavanagoudaPatil [5]. To relay the data packets from the source to the destination, the AODV routing protocol is used. Therefore, to reduce packet loss across the network, the Prevention of Selfish Node utilizing Hash Function (PSNHF) with location update algorithm is suggested.

A revolutionary Quality of Service based protected multi-path routing scheme is proposed for efficient data communication along with encryption technique [6]. Rajashanthi, M., Valarmathi, K.[6] The AODV-BR protocol with Optimal Fuzzy Logic is also built for the multipath routing phase. The Grey Wolf Optimization Adaptive Formation method envisions the optimum course.

An ideal route is then selected from the known routes to secure the techniques of data key management; Homomomorphic Encryption is used here. In terms of criteria such as end-to-end latency, packet distribution ratio etc., the productivity in the functioning of the expected methodology is measured.

In MANETs with congestion perception, Reddy, A. P., & Satyanarayana, N.[7] suggest a method known as reliable and secure multipath routing. Bandwidth is the goal of this strategy, and latency is taken into consideration while routing. In this method, the residual energy and reliability of the connections in the network are estimated by the network. It also calls the receiving energy and the transmission energy of the node when calculating the residual energy. The stability of the LET connection is then calculated; this LET is obtained using motion parameters (i.e. velocity, direction of the nodes). The network chooses the route to relay the data packets between the nodes depending on these criteria.

Banoth Rajkumar, Gugulothu Narsimha[8] suggests safe multi-path routing and data transfer where RREQ packets are signed for route discovery using digital signatures. As the destination collects the first RREQ packets from the server, all signatures are checked by the destination and the path list is cached by the source node session key. Then, it sends the RREP to the source node using the same direction. If the signature has been checked, the route is approved. The message components are encrypted at the source node using session keys and the hash function. Safe routing may be achieved depending on the confidence level of the nodes. To select an optimum safe routing route, an algorithm was used. The messages are then split into four bits, gently encrypted, and XOR operations are conducted. Lastly, the target node decrypts the initial message and restores it.

G. V. Madhu Viswanatham, S. G. N. Anjaneyulu and B. Venkateswarlu[9] The key emphasis of this paper is on authentication and secrecy during data transfer between MANET nodes. To provide security and strengthen data protection, we suggested a novel solution. A transmitting signature scheme built to use the issue of polynomial symmetrical decomposition dependent on non-commutative division seedlings. The principle is to combine the framework of signatures and multipath routing. And if an intruder happens to get one or more transmitted pieces, the likelihood of restoration of the original message is almost zero.

Received 20 January 2021; Accepted 08 February 2021.

Dr. D. Jagadeesan, G. Asha, M. Geetha, Dr. S.K. Srivatsa[10] Multipath routing is a commonly employed method in the Mobile Ad Hoc Networks for utilising many alternate routes (MANETs). Message transmission in multipath routing is split into streams and is transmitted along different routes. There could be a risk of loss in the direction during the delivery of the packet. In order to resolve this setback, an alternate route must be chosen to effectively send the message stream. Based on the latest ERS (Effective Route Selection) criterion, which requires maximum usable bandwidth and minimal transmitting period, the efficient alternate path is chosen. The proposed parameter is introduced in the Network Simulator (NS-2) and is evaluated for performance. The new ERS parameter selects an effective, bandwidth-increased alternative route and increases network efficiency.

3.Comparison of Secure Multipath Routing Methods

S. No	Authors	Algorithm	Merits	Demerits
1	Veeraiah, N., Krishna, B.T[1]	Multipath routing is carried out on the basis of the proposed BSWOA, which fixes the main disadvantages involved with conventional multipath routing strategies. BSWOA, which is the incorporation of the regular WOA into BSA, which inherits the advantages of WOA into BSA, is the foundation of safe routing.	The proposed BSWOA obtained the maximum energy, efficiency, detection rate and minimum delay	With the introduction of the Intrusion Response Framework (IRS) with a hybrid response strategy, the suggested system can be further enhanced.
2	Borkar, G.M., Mahajan, A.R[2]	The Dolphin Echolocation Algorithm for successful communication in MANET proposed mesh dependent multipath routing scheme to discover all feasible protected paths using secure adjacent place confidence verification protocol and better connection optimal	The suggested routing protocol creates a stronger packet distribution ratio, eliminates packet delays, reduces overheads and offers protection against bugs and threats.	The need to work on further threats

		path finding.		
3	A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba[3]	A modern energy-efficient multipath routing algorithm called FF-AOMDV has been proposed. Three separate situations, different node velocity, packet size, and time of simulation. Five (5) success measures have evaluated those situations (Packet delivery ratio, Throughput, End-toend-delay, Energy consumption and Network lifetime).	In several of the network efficiency indicators and criteria, the suggested FF-AOMDV outperformed AOMDV and AOMR-LM.	Not sufficient for complex networks
4	H. R. Jain and S. K. Sharma[4]	There is an adaptive strategy in the proposed solution in which our proposed scheme is more energy efficient. The filtering forwarding method slows down the spread of excessive RREQs created by a node per unit time and prevents denial of service attacks with success.	The energy usage of the network is lower and our network becomes more robust, and the proposed strategy has a higher packet distribution ratio and increased throughput.	Unable to apply for more no of attacks
5	MallikarjunaAnantapur,VenkanagoudaChanabasavanagouda Patil[5]	In AODV, the hash function is used to encrypt the transfer of data from the source to the destination. The AODV routing protocol's higher speed and lower computing characteristics are used to find an appropriate way to transfer data across the network. When conducting the route discovery method, the AODV-PSNHF technique prevents the selfish node. This method of AODV-PSNHF offers secure and healthy	In terms of energy usage, throughput, Packet Distribution Ratio (PDR), packet failure and normalised routing load, the effects of the proposed AODV-PSNHF system are evaluated.	Need accuracy in detection of selfish nodes.

		transmission of data under selfish nodes		
6	Rajashanthi, M., Valarmathi, K.[6]	For efficient data transmission along with encryption techniques, a Quality of Service (QoS) based safe multipath routing scheme was suggested. A route may lose its communication quality following the amount of transmissions. In terms of end-to-end delay, packet distribution ratio, resources, and throughput, the role of the projected strategy was related to the organisations available. It is possible to verify and equate the performance of the proposed protocol with current techniques. Finally, for security purposes, we have conceived a Homomorphic encryption method.	The outcome of the simulation indicates that our proposed work develops energy quality and network lifespan rather than that of current work.	Need more focus on QoS and Delay
7	Reddy, A. P., & Satyanarayana, N.[7]	In MANETs with Congestion Perception, a method known as Effective and Secure Multipath Routing was proposed. The remaining energy and reliability of connections in the network are estimated by the network. It also calls the receiving energy and the transmission energy of the node when calculating the residual energy. Connect LET stability is estimated; this LET is accomplished by using motion	Based on all these variables, the best route can be picked during the routing phase. In addition, on the network, the battery level of the nodes may be taken care of. This results in strong success and high productivity of the network.	Need more focus on energy consumption

		parameters such as node velocity and path.		
8	Banoth Rajkumar, Gugulothu Narsimha [8]	Proposed a safe multipath routing and data transfer in MANET in which digital signatures are used along with RREQ messages to improve the protection such that the signatures are checked by the destination nodes. Then, safe route exploration is conducted dependent on the path duration and trust value of node. After path exploration, data transfer is started. During data transfer, soft encryption and XOR operations are done. The destination node on receiving the message will decode and retrieve the original message	Simulation result show that the proposed approach can improves the packet delivery ratio with reduced delay, packet drop, and resilience	Need to focus on efficiency
9	G. S. G. N. Anjaneyulu, V. Madhu Viswanatham and B. Venkateswarlu[9]	Provided a notion to transfer the data across multipaths between nodes in ad hoc network to improve the robustness of data confidentiality through safe authentication utilising digital signature principle.	Effective method for security and multipath routing	Need more focus on security issues
10	Dr. D. Jagadeesan, G. Asha, M. Geetha, Dr. S.K. Srivatsa[10]	In this article, a multipath routing protocol for efficient Route Selection in Mobile Ad hoc Networks is suggested. It prevents regular collisions and deterioration in the network efficiency.	By simulation results, we demonstrate that the proposed solution boosts network efficiency	Need more focus on life time of the network

4.The need for security in multipath routing in MANET

Routing is the fundamental operation in MANETs that enables the establishment of contact ties between sensor nodes and the packet delivery. Much of the protection core areas such as protected data aggregation, secure localization, intrusion prevention, key management, etc., depend on routing schemes to share data and sustain their service. Routing pathways are typically defined using a single route between the source and destination nodes. While this scheme is well adapted in MANETs where resources are scarce, failure of nodes along the route will imply failure of the path and loss of data. Furthermore, breaching the routing process will impact all other operations that depend on routing to provide their services. Loss of data is inappropriate in vulnerable places such as in military and healthcare settings, where their mission is strongly depended on details. Therefore, availability of data and continuity of contact are a must. Different methods have been developed to provide several directions in order to improve the availability, flexibility and stability of the network and assist in a timely critical decision making. Multiple routes suffer the same vulnerabilities as in single-path routing. However, the usage of several routes raises new protection issues that must be taken into account. For vulnerable settings, it is equally essential to safeguard data against unauthorizedbehavior as well as ensuring the availability and efficiency of the network. Therefore, protecting the multipath routing mechanism is a critical activity to ensure the efficient execution of the routing activities. However, prior to developing reliable routing protocols, one must consider the factors that contribute to the need for protection in the multipath routing phase. Only then researchers would be able to resolve the necessary protection criteria in their design.

Protection dependent on the Data redundancy. Multipath routing introduces traffic consistency in the network as a redundant routing technique is implemented by forwarding the same packet over a variety of different routes. With redundant routing, data are accessible at several locations providing further opportunity to adversaries to decrypt the details. Because several instances of a packet are traversing the network, the adversary has a greater chance of damaging packets by targeting multiple nodes. This is inappropriate in sensitive systems, because if vital data is detected or changed it may cause disruption to the application’s activity and even risk human lives.

Protection centered on Routing threats. Many routing protocols introduced in MANEs have not been developed with protection specifications in mind. Several multipath schemes have been suggested to provide efficiency of the connection formed in a MANET. However, in a protection sense, this is not enough as an attacker can always breach some, or all, of the paths and access the knowledge shared. Several threats have been thoroughly studied in the literature that can be launched against routing. In multipath routing, attacks will significantly influence the route discovery process and provide the ability to the adversary to monitor the alternate path establishment. Attacks may influence the route exploration process in various ways. A selective forward or a denial-of-service attack can prevent the discovery of all possible paths and thus monitor the network's connectivity. A hello or sybil attack can enable the adversary to engage in various routing paths and in this way compromise data travelling over the alternate paths. Much worse, the adversary may overhear the correspondence between nodes and change routing control packets affecting the exploration of alternate routes and generating routing loops and dead ends. Through gaining power over the routing process, the adversary will bring down the whole network.

Protection dependent on Survivability. Since batteries are the primary source of energy in MANETs, one of the main goals is for the network to operate in an optimal manner in order to prolong its lifespan as long as possible. This is much more essential particularly because MANETs may be implemented in remote or aggressive areas, rendering infeasible the tracking and replacement of the batteries. Multipath itself incurs more energy usage than single-path navigation. An attacker will launch security attacks in multipath routing protocols with the goal of taking advantage of the path/packet recovery mechanisms introduced by the protocol to obtain a higher energy consumption. Through targeting multiple nodes and sacrificing credibility, falling packets, etc., the adversary causes recovery mechanisms to be initialized on the node/network to solve the problem. As redundant routing is used, recovery may contribute to increased energy usage, for example, by resending the packet to all alternate paths and increasing the connectivity between sensor nodes. Through continuously initiating the attacks, the adversary will succeed in draining the batteries of any of the sensors at a rapid rate; this could contribute to the weakening of the routing mechanism and the network's efficiency, and ultimately result in the network's partition, preventing the application from running successfully. All the explanations point to the fact that protecting the multipath routing mechanism is of considerable

Received 20 January 2021; Accepted 08 February 2021.

importance. Prevention and recovery strategies can be utilized to facilitate in the network's failure tolerance and further support of its survivability. It is therefore important to ensure that all alternate routes have trustworthy nodes to forward packets, that an integrity breach is determined as early as possible to prevent unwanted contact and that a protection association scheme is implemented to confine risk to a local region in case cryptographic content is breached. Otherwise, possible changes or other sort of abuse of the routing data may trigger the nodes to become inaccessible, the network to act randomly and even cause the program to run in a dangerous way.

6.Proposed Approach

The developed secure conscious routing protocols are not successful due to high energy consumption and high communication overhead. The suggested approach would be mentioned problems are solved efficiently utilizing multipath routing that allows multiple routes to a destination. Thus, based on the design and nature of the MANETs, several powerful algorithms are required that better insist on the design of the multipath routing protocols. Source nodes, along with the middle nodes, utilize these routes as backup and primary routes. At present, the research group focuses on the exploration of the multipath to degrade the single-path issues, including higher latency in case of finding the directions, attempting often for discovering the roads, and possible enhancement in throughput during the data transmission. However, there are no such methods to degrade the above-mentioned problems connected with the multipath usage belonging to the on-demand routing protocols. The most significant function of this domain is multipath, which forwards the messages to multiple recipients from a server. Thus, the designed multipath routing protocol will address the above challenges.

7.Conclusion

In this paper, we have evaluated the state-of-the-art of stable multipath routing protocols in MANETs and discussed several security issues related to multipath routing itself. The protocols have been categorised depending on their security purpose and the security implementation approach they adopt. There are protocols that aim in securing the multipath routing procedure itself. Other protocols are designed to detect and recover from specific attacks while others support the operation of other secure areas in MANETs. We have also overviewed the protection criteria of sensitive applications that use MANETs and say that mission-critical applications place priority differently than what shapes the traditional security requirements chain. We have listed the reasons that drive the need for security in multipath routing cultivating a better understanding of the threats that exist. Finally, we discuss future directions and straightforward challenges. As future research, we plan to design an appropriate appraisal framework, based on which a spherical procedure evaluation and comparison can be established.

References

1. Veeraiah, N., Krishna, B.T. “An approach for optimal-secure multi-path routing and intrusion detection in MANET”,Evol. Intel. (2020).
2. Borkar, G.M., Mahajan, A.R. “A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks”, Wireless Netw**23,** 2455–2472 (2017).
3. A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function", in IEEE Access, vol. 5, pp. 10369-10381, 2017.
4. H. R. Jain and S. K. Sharma, "Improved energy efficient secure multipath AODV routing protocol for MANET", 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India, 2014, pp. 1-9.
5. MallikarjunaAnantapur,VenkanagoudaChanabasavanagouda Patil “Position Update Secure Routing protocol for MANET”,International Journal of Intelligent Engineering and Systems, Vol.14, No.1, 2021.
6. Rajashanthi, M., Valarmathi, K. “A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs”,Wireless Pers Commun**112,** 75–90 (2020).
7. Reddy, A. P., & Satyanarayana, N. (2017). “Energy-efficient stable multipath routing in MANET. Wireless Networks”,23(7), 2083–2091.
8. Banoth Rajkumar,Gugulothu Narsimha “Secure multipath routing and data transmission in MANET”,Int. J. Networking and Virtual Organisations, Vol. 16, No. 3, 2016.
9. G. S. G. N. Anjaneyulu, V. Madhu Viswanatham and B. Venkateswarlu “Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks”,Advances in Applied Science Research, 2011, 2 (4):177-186.

10. Dr. D. Jagadeesan, G. Asha, M. Geetha, Dr. S.K. Srivatsa “Effective Route Selection Based on Transmission Time and Bandwidth for Multipath Routing in MANETs”, International Journal of Computer & Organization Trends –Volume 5 Issue 2 March to April 2015.
11. 13. Li J, Lewis HW (2016) “Fuzzy clustering algorithms – review of the applications” In: Proceedings of the IEEE international conference on smart cloud (SmartCloud), pp 282–288.
12. Singh O, Singh J, Singh R (2018) “Multi-level trust-based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET”, Cluster Comput 21:51–63.
13. Subba B, Biswas S, Karmakar S (2016) “Intrusion detection in mobile Ad hoc Networks: Bayesian game formulation”,Eng Sci Technol 19(2):782–799 .
14. Yadav AK, Tripathi S (2017) “QMRPRNS: design of QoS multicast routing protocol using reliable node selection scheme for MANETs”, Peer PeerNetw Appl 10(4):897–909.
15. Chaudhry R, Tapaswi S (2018) Optimized power control and efficient energy conservation for topology management of MANET with an adaptive Gabriel graph. ComputElectrEng 72:1021–1036
16. Xian-Bing Meng XZ, Gao LL, Liu Y, Zhang H (2016) “A new bio-inspired optimisation algorithm: bird swarm algorithm”, J Exp TheorArtifIntell 28(4):673–687 .
17. Mirjalili S, Lewis A (2016) “The whale optimization algorithm”, Adv EngSoftw 95:51–67
18. Marchang N, Datta R, Das SK (2017) “A novel approach for efcient usage of intrusion detection system in mobile ad hoc networks”, IEEE Trans Veh Technol 66(2):1684–1695.
19. Pi S, Sun B (2012) “Fuzzy controllers based multipath routing algorithm in MANET”,Phys Procedia 24(Part B):1178–1185.
20. Mohapatra P, Li J, Gui C (2009) “QoS in mobile ad hoc networks”, In: Proceedings of the IEEE 10th annual conference on wireless and microwave technology, vol 10, no 3, pp 44–53