ISSN 2394-739X

IJRSET NOVEMBER Volume 10 Issue 11

International Journal for Research in Science Engineering & Technology (IJRSET)

https://www.doi.org/10.5281/zenodo.10212336

EXPLORING SECURITY AND ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS: A COMPREHENSIVE REVIEW

[1] Mrs. P. Vidhya Devi, [2] Dr. B. L. Shivakumar
[1] Assistant Professor, [2] Principal,
[1, 2] Department of Artificial Intelligence & Data Science,
[1, 2] Sri Ramakrishna College of Arts & Science, Coimbatore,
Tamil Nadu, India.

ABSTRACT – Mobile ad hoc networks (MANETs) are autonomously self-coordinated networks without infrastructure support. MANET works under no proper infrastructure in which each hub works loves a switch that stores and advances parcel to conclusive destination. Because of its dynamic topology, MANET can be made anyplace, whenever. As there are restricted assets in MANET so it deals with numerous issues like security, restricted transfer speed, reach and power constraints. This paper surveyed various strategies to manage congestion control, security issues, various layers assaults, routing protocols and difficulties that are looked by MANET.

Keywords: [MANET, Proactive and Reactive routing protocols, Unicasting, Ad-hoc network;]

1. INTRODUCTION

Mobile Ad Hoc Network (likewise called MANET) MANETs are self-determining, self-maintained, and self-healing, taking into account outer network adaptability. It is a network of mobile routers associated by remote connections - the association of which shapes an impromptu topology. The routers are allowed to move arbitrarily and arrange themselves aimlessly; in this manner, the network's remote topology would change quickly and unsure. This kind of network might work in an independent manner, or would be associated with the bigger Web. Nodes in these networks will both create client and application traffic and do network control and routing protocols. Quickly evolving connectivity, network allocations, most extreme error rates, collision conflicts, and bandwidth and power constraints together posture new issues in network control especially in the plan of more significant level protocols, for example, routing and in executing applications with Nature of Service prerequisites. Mobile applications present additional challenges for network networks as changes to the network topology are swift and widespread. In a mobile ad hoc network, nodes move readily; thusly the network might encounter quick and flighty topology changes. Since the nodes in a MANET regularly have restricted scope of transmission, a few nodes can't discuss straightforwardly with one another. Thus, routing tracks in mobile ad hoc networks possibly contain various hops, and each hub in mobile ad hoc networks has the obligation to perform like a router. Not at all like gadgets in traditional Remote LAN arrangements, all nodes are mobile and the topology of the network is changing progressively in an Ad Hoc Networks, which carries huge and extraordinary challenges to the security of Ad Hoc Networks.

2. LITERATURE SURVEY

1. Albers (2002) et.al proposed a distributed and collaborative architecture of IDS by using mobile agents. Local Intrusion Detection System (Covers) operates on individual nodes, sharing security and intrusion data with Tops for global awareness. Covers may run on diverse systems, complicating data integration. Using SNMP data in MIBs as a standardized source can streamline data management and reduce resource overhead. Combining anomaly and misuse detection enhances the IDS, enabling Tops to respond and secure the network against detected intrusions.

Merits

If all Covers in a community have comparable detection capacities, scalability of the community's global IDS is ensured.

Demerits

Mobile specialists give answers for the generally low exhibitions of Manets and their utilization make the global architecture evaluative.

2. P Patel (2016) et.al proposed Performance Evaluation of MANET Network Parameters using AODV Protocol for HEAACK Enhancement. The Enhanced Adaptive Acknowledgment (EAACK) intrusion detection system enhances security in Mobile Ad-hoc Networks (MANETs) by detecting malicious nodes and countering fake reports. EAACK has low routing overhead (0.58%) and high packet delivery ratio (0.92%) even with over 40% malicious nodes, preventing network partitioning. Hybrid Enhanced Adaptive Acknowledgment (HEAACK) adds cryptography like RSA and Triple DES for improved security and reduced data manipulation and network overhead.

Merits
Ad-hoc networks are outstandingly useful explanation and easy to convey requires less manual intervention since there are no links included.

Demerits
The open medium and remote appropriation of MANET make it defenceless against different sorts of attacks.

3. Sangeetha (2017) et.al proposed an efficient Self Organized Gradient Boosting Key Authentication (SOGBKA). SOGBKA enhances MANET data communication security and throughput by using Gradient Boosting trees to create self-coordinated keys for nodes. Trust values are computed based on packet send and drop rates, facilitating tree pruning to eliminate low-trust nodes. The method improves data delivery reliability, achieving high security through self-coordinated key authentication. It outperforms existing techniques.

Merits
SOGBKA technique accomplishes tree pruning which leads to kill the mobile node with lower trust value.

Demerits
Further fostering the throughput rate and decreasing time taken failed to remember data conveyance in MANETs.

4. Arepalli (2016) et.al proposed Secure Multicast Routing Protocol in MANETs Using Efficient ECGDH Algorithm. A Mobile Ad-hoc Network (MANET) is a self-reliant, dynamic communication network of mobile nodes without fixed infrastructure. It's crucial for group communication in applications like military and emergency operations. Despite security challenges, PUMA is a top multicast routing protocol. To counter Man-in-the-Middle attacks, ECGDH was introduced, enhancing security and maintaining efficiency even after an attack.

Merits
PUMA routing protocol under the ordinary circumstance, under an attack situation and guarding with ECGDH security.

Demerits
A Mobile adhoc network is an infrastructure less network that has no trusted authority.

5. Echchaachoui A (2014) et.al proposed Asymmetric and dynamic encryption for routing security in MANETs. This paper proposes a novel approach to enhance security and performance in Ad-hoc networks, focusing on mobile ad-hoc networks characterized by dynamic topologies. They employ asymmetric encryption, clustering, and the OLSR-SDK protocol to defend against Black Hole and DDOS attacks. Results show significant traffic performance improvement and reduced delay, with plans to strengthen resistance against data destruction attacks.

Merits
OLSR-SDK, giving an elevated degree of security, has extraordinarily further developed traffic performance against a DDOS attack that straightforwardly target nodes.

Demerits
Providing an improvement of 32% however didn't further develop packet delivery rate.

6. Sun B (2008) et.al proposed multiple constraints QoS multicast routing optimization algorithm in MANET based on GA. In mobile ad hoc networks, no static infrastructure exists, requiring message relay through intermediate nodes when nodes are out of radio range. These networks serve military, emergency, and policing purposes but have unpredictable topologies due to node mobility and limited bandwidth. To address this, a genetic algorithm-based MQMGA ensures QoS in multicast routing for improved connection usage, cost, path longevity, delay, and reliability in dynamic mobile networks. Experimental results demonstrate its effectiveness.

Merits
Efficient technique for assessing and assessing the route stability in dynamic mobile networks.

Demerits
The development of cost to control information is lower, and not causes the flooding storm.

7. Yang F (2012) et.al proposed Network coding-based AOMDV routing in MANET. MANET, a self-organizing network without infrastructure, relies on multipath routing for reliability. Multipath utilizes node density for stable communication. Network Coding-based AOMDV (NC-AOMDV) enhances data transmission and load balancing. In simulations, NC-AOMDV outperforms AODV in packet delivery, overhead, and end-to-end delay assessment, ensuring dynamic MANET robustness.

Merits
The NC-AOMDV routing algorithm can be handily extended to other mobile networks QoS routing issues with NP intricacy.

Demerits
The packet delivery proportion diminishes as the node's portability speed increments.

8. Duraipandian M (2019) et.al proposed Performance evaluation of routing algorithm for Manet based on the machine learning techniques. Advancements in wireless communication have boosted mobile ad hoc networks, which rely on mobile nodes for infrastructure-free networking. Nodes move freely, self-organize, and act as hosts and routers. This paper introduces a reinforcement learning-based routing strategy to optimize energy use, reduce transmission delay, and enhance packet delivery, tested in Network Simulator-II for efficiency.

Merits
The correlation with the common strategy shows the proficiency of the proposed technique over the predominant.

Demerits
The security issues in the short way foundation for the mobile adhoc networks.

9. Sharma B (2014) et.al proposed Energy efficient load balancing approach to improve AOMDV routing in MANET. A Mobile Ad hoc Network (MANET) is a self-organizing network without fixed infrastructure, where mobile nodes act as hosts and routers. To address shortcomings in existing multipath routing protocols, a new approach called Energy-Based Multipath Routing (E-AOMDV) is proposed, which combines shortest path, load balancing, and energy conservation, improving network performance and lifetime.

Merits
If the load is appropriately circulated then, at that point, all things considered energy usage increments and diminishes energy consumption.

Demerits
Dividing the network into a number of regions that differs dynamically based on the node portability pattern.

10. Kaur S (2015) et.al proposed Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature. Mobile Ad hoc Networks (MANETs) are gaining popularity due to their infrastructure independence, but security remains a significant challenge. Symmetric key algorithms are favoured for their efficiency and power-saving properties. RSA, a widely used public-key cryptosystem, can enhance MANET security. This paper aims to simplify the RSA algorithm and implement it in MANETs, comparing it with a modified AODV protocol for performance evaluation.

Merits
In MANET, each and every node goes about as both host and router. That is all there is to it is self-determining in conduct.

Demerits
There is no centralized administration control, so finding the ways between nodes is troublesome.

11. Ahmad A. (2018) et.al proposed User selective encryption method for securing MANETs. Addressing MANET security challenges is crucial due to their vulnerability to attacks and limited resources. Lightweight and storage-efficient key management is essential. This paper proposes a client-specific encryption method using DES, 3DES, AES, and DHKE to enhance MANET security. Through NS-2 simulations, AES demonstrates superior performance in data transfer time and network throughput across various data sizes and hop counts, validating the proposed approach's effectiveness compared to prior studies.

Merits
The MANET client the capacity to dynamically pick the favored encryption conspires based on the security level required.

Demerits
The reasonableness of the cryptographic solutions with Ad hoc limits will constantly be testing.

12. Khan A (2017) et.al proposed Energy efficient partial permutation encryption on network coded MANETs. The proposed partial permutation encryption scheme improves security efficiency in MANETs by selectively permuting GEVs, reducing computational complexity and energy costs. It features dynamic key generation for enhanced security; achieving 117% better throughput compared to Blowfish and significantly lowers energy consumption, making it ideal for energy-constrained devices.

Merits
The proposed contrive has multiple times lesser energy utilization than the Blowfish algorithm that makes it a useful encryption method for energy limitation contraptions.

Demerits
The fundamental issue in the regular routing approach is featured when a message is communicated through a number of middle nodes.

13. Minghu Wu (2010) et.al proposed Data security in MANETs by integrating multipath routing and secret sharing. In secure routing protocol, the fundamental issue is to safeguard our communicated Propose a secure multipath routing strategy that combines secret sharing, considering various metrics like hop count, traffic load, node centrality, and link reliability to enhance data security and transmission efficiency. Also, incorporate hash functions for detecting dynamic attacks. Simulations demonstrate the scheme's effectiveness in ensuring both security and performance.

Merits
The re-enactment results show that protocol keeps up with sensible tradeoff among security and performance proficiency.

Demerits
Multipath routing consumes more network asset, however if by some stroke of good luck not cost gigantic energy.

14. V. S. Bhargavi (2016) et.al proposed Enhancing security in MANETS through trust-aware routing. A Mobile Ad Hoc Network (MANET) is a self-forming wireless network where all nodes also function as routers. This proposed protocol enhances security by having source nodes evaluate node authenticity based on trust values gathered from the network. This ensures a secure transmission path, improving packet delivery, throughput, and reducing delays and overhead, even in the presence of malicious nodes, addressing challenges like wormhole and black hole attacks.

Merits
Various kinds of measurements can likewise be utilized to settle on a nodes authenticity to accomplish better and greater security when more number of malicious nodes is available.

Demerits
MANET's likewise result in successive changes in the area of the mobile nodes which makes routing task more convoluted.

15. G. Thandavaraya (2012) et.al proposed ORZEF: An optimized routing using zone to establish security in MANET using multipath and friend-based ad hoc routing. Mobile Ad Hoc Networks (MANETs) are decentralized wireless networks prone to attacks. This system ensures strong security by symmetric key exchange, making it difficult for malicious nodes to compromise data. Challenges and periodic key exchange expose malicious nodes, preventing resentment wars. Multipath routing is used when few trusted nodes are available, reducing overhead and enhancing security. This dynamic protocol makes the system efficient.

Merits

This then again lessens overheads and thus decreases the possibilities of unsecured routing through malicious nodes.

Demerits

Challenges and symmetric key exchange are periodic progression where data transmission by nodes is on demand.

CONCLUSION

In this paper, introduced a review of various Security issues, assaults on physical, information and organization layers and furthermore give security solutions. Different routing protocols examined in the paper are extremely useful and viable for new specialists to recognize recent concerns for advance exploration. This paper reviewed different systems to manage congestion control, security issues, different layers attacks, routing protocols and troubles that are looked by MANET.

REFERENCES

[1]. Albers P, Camp O, Percher JM, Jouga B, Me L, Puttini RS. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In Wireless Information Systems 2002 Apr 3 (pp. 1-12).

[2]. Sun B, Pi S, Gui C, Zeng Y, Yan B, Wang W, Qin Q. Multiple constraints QoS multicast routing optimization algorithm in MANET based on GA. Progress in Natural Science. 2008 Mar 10; 18 (3):331-6.

[3]. Yang F, Ling S, Xu H, Sun B. Network coding-based AOMDV routing in MANET. In2012 ieee international conference on information science and technology 2012 Mar 23 (pp. 337-340). IEEE.

[4]. Duraipandian M. Performance evaluation of routing algorithm for Manet based on the machine learning techniques. Journal of trends in Computer Science and Smart technology (TCSST). 2019 Sep; 1(01):25-38.

[5]. A. Echchaachoui, A. Choukri, A. Habbani and M. Elkoutbi, "Asymmetric and dynamic encryption for routing security in MANETs," 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 2014, pp. 825-830, doi: 10.1109/ICMCS.2014.6911237.

[6]. Sharma B, Chugh S, Jain V. Energy efficient load balancing approach to improve AOMDV routing in MANET. In2014 fourth international conference on communication systems and network technologies 2014 Apr 7 (pp. 187-192). IEEE.

[7]. Kaur S, Kaur H. Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature. International Journal for Advance Research in Engineering and Technology. 2015; 3:24-8.

[8]. Arepalli G, Erukula SB, Gopi AP, Nagaraju C. Secure Multicast Routing Protocol in MANETs Using Efficient ECGDH Algorithm. International Journal of Electrical & Computer Engineering (2088-8708). 2016 Aug 1; 6(4).

[9]. Sangeetha MS, Sathappan S. Self Organized Gradient Boosting Key Authentication for Secured Data Communication in Mobile Ad-hoc Network. International Journal of Applied Engineering Research. 2017; 12(18):7823-32.

[10]. Patel P, Bansode R, Nemade B. Performance evaluation of MANET network parameters using AODV protocol for HEAACK enhancement. Procedia Computer Science. 2016 Jan 1; 79:932-9.

[11]. Ahmad A, Ismail S. User selective encryption method for securing MANETs. International Journal of Electrical and Computer Engineering (IJECE). 2018 Oct; 8(5):3103-11.

[12]. Khan A, Sun QT, Mahmood Z, Ghafoor AU. Energy efficient partial permutation encryption on network coded MANETs. Journal of Electrical and Computer Engineering. 2017 Apr 6;2017.

[13]. Minghu Wu, Siguang Chen and Jiaping Liao, "Data security in MANETs by integrating multipath routing and secret sharing," 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010), Wuhan, China, 2010, pp. 72-75, doi: 10.1109/CAR.2010.5456776.

[14]. V. S. Bhargavi and S. V. Raju, "Enhancing security in MANETS through trust-aware routing," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 1940-1943, doi: 10.1109/WiSPNET.2016.7566481.

[15]. G. Thandavarayan, K. Sangeetha and S. Seerangan, "ORZEF: An optimized routing using zone to establish security in MANET using multipath and friend-based ad hoc routing," International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), Salem, India, 2012, pp. 221-224, doi: 10.1109/ICPRIME.2012.6208347.