

Security Issues and Minimax-Based Optimal Approaches for Mobile Ad Hoc Networks

Aarti Sehwag¹, Nrusimhadri Naveen², Jyoti Gupta³, Deepika Yadav⁴, Amrita Ticku⁵, Akanksha Kochhar⁶

¹Department of Computer science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi. Email id: aarti@Bharativedyapeeth.edu

²Phd Research scholar, Shri venkateshwara university, Gajraula, UP.
Email: naveenbtechcse@gmail.com

³Assistant Professor, Department of Electronics and Communication Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi. Email id: jyotig1989@gmail.com

⁴ Assistant professor, Department of Computer science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi.

⁵ Assistant professor, Department of Computer science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi. Email: amrita.ticku@Bharativedyapeeth.edu

⁶ Assistant professor, Department of Computer science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi. Email: akanksha.kochhar@bharativedyapeeth.edu

Abstract

To offer secure communication between mobile nodes in the hostile environment, security has turned into a top priority. The distinctive features of mobile ad hoc networks, as opposed to wireline networks, present a variety of nontrivial problems to security design and data in transit. These difficulties amply demonstrate the need for developing multifaceted security solutions that deliver both effective security and optimal network performance. The main aim of this study is to identify and discuss the security challenges and potential defence approaches against security attacks in ad hoc and mobile networks. The study recognises that key build encryption system as an effective method foreseeing advanced hybrid developments to secure the mobile ad hoc systems.

Keywords: *Mobile ad hoc network, Network Security, Intrusion, Secure ad hoc network*

1. Introduction

Mobile Ad hoc network, also known as MANET, refers to a collection of self-configuring, multi hop wireless networks that are free to manoeuvre location and configure themselves [1]. MANET rely on wireless connections for communication with other networks due to their mobility. MANETs are more vulnerable to assaults as they are connected to wireless networks. In order for MANETs to have a successful deployment and usage, multiple levels of assurances need to be provided to different applications. Due to the ease with which anybody can utilise the network resources, security assaults on data transmission and accessibility are common, including passive eavesdropping, packet injection, and unauthorized disclosure[2].

Nodes need to be incorporated into the routing condition in order to prevent these kinds of attacks, and which will protect mobile Ad-hoc networks from being subjected to a wider variety of potential threats[3]. Several optimal approaches have been reported to enhance the network security in MANET. This study aims to identify the potential security challenges and defence approaches against security attacks in mobile ad hoc networks. Further, the identified optimal approaches will be discussed, and the efficient approach will be comprehended for future advancements.



Figure 1: Mobile Ad hoc network structure[4]

2. Security challenges in mobile ad hoc network:

A mobile ad hoc network structure is accomplished primarily through the protocols of link-layer, which ensure connectivity over a single hop, as well as the protocols for network-layer, which extend connectivity over multiple hops. The data packet forwarding and Ad hoc routing are the primary network-layer functions in MANETs[5]. These two processes interact with one another and are responsible for the functionality of transporting data packets from their point of origin to their final destination. The protocols for Ad hoc routing allow for the exchange of the routing messages among the nodes and the maintenance of the routing states at every node in accordance with these messages. Data packets are moved along the established route to their destination by intermediary nodes, and this movement is determined by the routing states. However, both the packet forwarding and routing activities are susceptible to malicious assaults, which can result in a wide variety of different kinds of malfunctions at the network layer. Any activity for the advertising routing changes that doesn't meet the standards of routing protocol is included in the family of routing attacks [6]. There is a connection between the particular attack behaviours.

The term *Man in the Middle* (MITM) was first used in the context of a basketball game, in which a player in the middle of the court attempts to steal the ball from two other players who are trying to pass it to each other. A method very similar to this one is utilised in MANET, in which MITM attackers put the communications of legitimate nodes at risk by modifying the information in transit. These kinds of assaults have severe repercussions for the communication, particularly when the content of the message includes instructions concerning how to manage the risks[7].

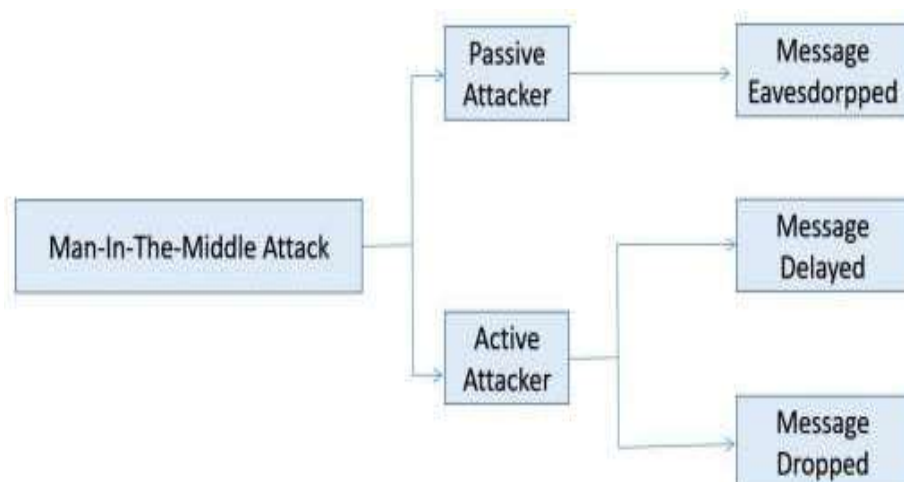


Figure 2: Man in the Middle attack in ad hoc network [8]

The *wormhole* attack is a common and serious security attack in ad hoc networking and other network security systems. This assault utilises two or more than two malicious nodes, and the data packets that are disseminated are those that have been tunnelled from one end of the malicious node to the other spiteful or malicious node at the other point. MANETs are more susceptible to wormhole attacks than other types of networks due to their high mobility and dynamic nature. During a wormhole attack, the attacker could sniff the packet data and retransmitting them results in a loss of throughput as well as infringe the bullying privacy[9].

3. Insights for security implementation:

Networking security framework is based on the physical security of the network's components. In addition, the fundamentals of the network security approach for mobile ad hoc networks have a significant impact on the relevance and potential consequences of the topic of physical security. For instance, in modern web-based intranets, firewalls, proxies, and any other centralised components that separate secure and non-secure domains are discrete vulnerabilities. As a result, it is important to ensure the physical security of such components[10].

The pre-set routing protocols do not use any form of security protection all through end-to-end type of communication. This is performed to ensure that the protocol can attain optimum network throughput in an environment that is consequently dynamic in nature. As a further outcome of frequently shifting membership and topology, the relationships based on trust relationships that exist between each individual node are of an extremely low quality. This results in numerous attacks which could be initiated against the network, providing hackers with a significant chance to induce themselves into the network as a cooperative nodes.

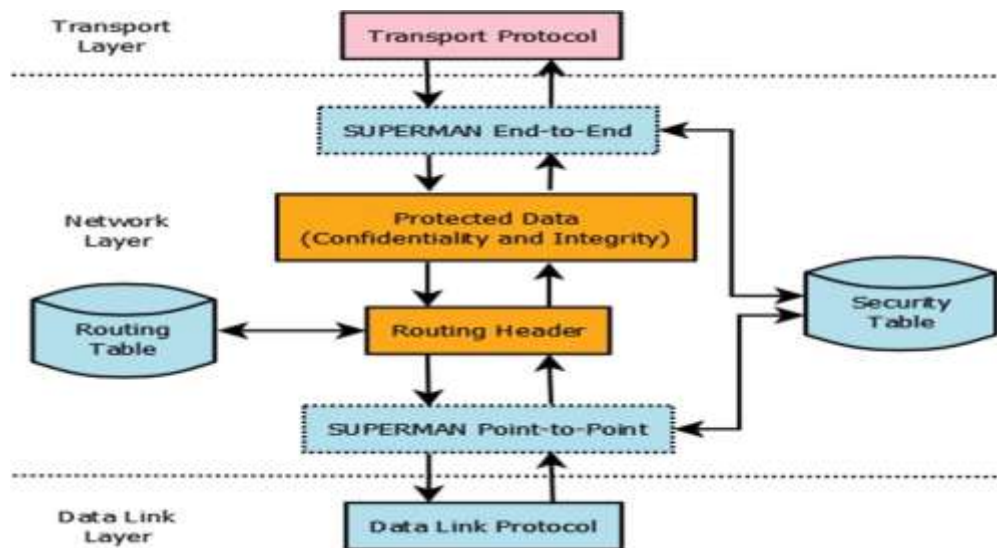


Figure 3: SUPERMAN routing technique for network security layer [11]

In light of numerous attacks, security protection used to guarantee the integrity of mobile ad hoc network might not only be capable to repel attacks from the outside, but it should also be able to prevent attacks from within the network that are initiated against network from any of the compromised node. The majority of security measures depends upon the data encryption, i.e., when a message and a secret key are combined to produce a ciphertext which can't be decrypted without the use of an original key [12]. By using this mechanism for encryption, it will be inconceivable for any unauthorised user to read the encrypted communication. However, if an adequate number of packets are captured it is possible to decipher a secret key that has been installed. Therefore, dynamically generating the secret key and periodically replacing it is the most effective way to defend network from these attacks. In addition, the protocol that is used for mobile ad-hoc type of wireless network must have enough flexibility to allow it to adjust to various security level protection in order to meet the requirements of applications operating in a variety of environments and making use of a wide range of communication speeds.

4. Significant Potential techniques:

The use of asymmetric key cryptography method, such as RSA, provides the foundation for *digital signatures*. Due to this, the signing/decrypting and verifying/encrypting processes require a significantly higher amount of computational overhead [13]. It has a lower resistance to denial-of-service attacks due to the fact that an attacker might flood the victim node with high number of fake signatures in order to use up all of the victim's computational resource while validating the signatures. In addition to this, each node is required to maintain its own certificate revocation list (CRL) of credentials that have been revoked. On the other hand, a digital signature might be authenticated by any type of node as long as that node is in possession of the signing node's public key. Digital signatures can be used with an extremely high number of receivers. Within a network consisting of n nodes, there is only a requirement to store a total (n) private/public key pairs[14].

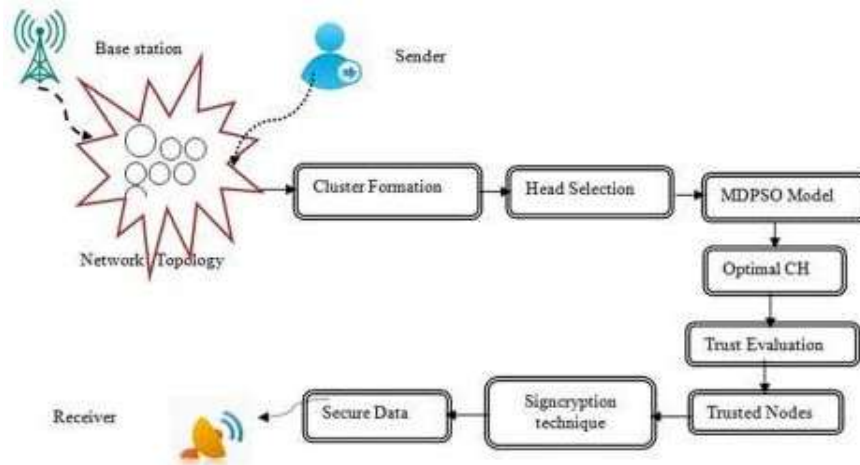


Figure 4: Signcryption, a digital signature model for mobile ad hoc network[15]

The proactive approach is used by the ad hoc and secure protocols, which also include enhancements to the already present protocols of ad hoc routing, like *Ad-hoc On-demand Distance Vector* (AODV) as well as *Dynamic Source Routing protocol* (DSR), that provide security extensions[16]. Within these protocols, every mobile node affirmatively signs the routing messages by utilising primitives for cryptographic authentication that were explained earlier. In this way, collaborative nodes are able to verify legitimate traffic in an effective manner and distinguish unauthenticated packets sent by outer attackers from legitimate traffic. However, even a trusted node could fall under an adversary's control if it was compromised.

An innovative statistically based solution that defends Mobile Ad hoc Network from the flooding assault was introduced for better security performance. In *security extension of the AODV* (SAODV), distribution is utilized as a statistical reason in exploring the node that is disordered due to an overload of Route Request (RREQ). This is done in order to find the best route through the network. The variation in the number of RREQs that were successfully completed by different Mobile Ad hoc Network nodes, is what is used to compute spreading. The MANET that operate below the AODV protocol can easily detect and avoid security attacks with the assistance of the method. The statistical threshold value serves as the foundation for this approach. This threshold value is dependent on the variation in RREQs produced by a large number of nodes in the MANET as well as the variation in RREQs produced by each and every mean[17].

For a hybrid system, the Ad hoc On-demand Multipath Distance Vector (AOMDV) protocol has been implemented for the discoveries of multiple routes. Additionally, the (KNN) K-Nearest Neighbor protocol has been implemented for the selection of nearest neighbour nodes, and the False key-build Advanced Encryption Standard (FAES) encryption scheme has been implemented as the cryptography method for security of the system. The goal of utilising the FAES algorithm is to protect the data and devices of the internet of things (IoT) from any hardware or network-based assaults. The FAES-AOMDV protocol assures the safe transfer of data while consuming the least amount of energy possible in an environment where malicious nodes may be present [18].

5. Limitation

Both authorised network users and malevolent attackers might access the wireless channel. As a direct consequence of this, there is no distinct line of defence in MANETs from the point of view of the security design. It is clearly not able to position the single security solution as there is no location or infrastructure that has been clearly specified. In addition, portable devices, along with the information regarding the system's security that they reserve, are susceptible to breaches. This is especially prevalent in low-end devices with inadequate protection. The compromised nodes in the affected devices, which represent the network's weakest link, make it possible for attackers to gain access to the network and set off a chain reaction of security holes throughout the system.

The security method used by MANET device needs to be compatible with the constraints imposed by its own resources, including those pertaining to its capacity for processing, memory, and communication. Each tier of the protocol stack must therefore contribute to a separate line of defence, which is why the security solution must encompass multiple layers of the stack. It is impossible to defend against all possible attacks with a solution that consists of only one layer. All of the three components for prevention, reaction and detection are required to be incorporated into the security system.

6. Conclusion

The above discussed identified and discussed on the significant security challenges and optimal approaches to enhance the security concerns in MANETS. The two most crucial security needs in the ad hoc network in the current developing era are security and privacy of the network and data in transit. The study concludes with a recognition that key build encryption systems exhibit prevalent implementation with remarkable adaptability and efficiency for hybrid improvements in futuristic approaches. The solutions have been explicitly designed with keeping in mind the targeted attack models, where they function well when those attacks were encountered but may not survive the unexpected intrusions. Hence, the security solution is suggested to be considered foreseeing for resilience along with a number of features.

Reference

- [1] A. Dorri and S. R. Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey," *Int. J. Comput. Sci. Eng. Surv.*, vol. 6, no. 1, 2015.
- [2] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile Ad hoc networks: a predictive approach," *Int. J. Inf. Technol.*, vol. 11, no. 2, 2019.
- [3] A. Guillen-Perez, A. M. Montoya, J. C. Sanchez-Aarnoutse, and M. D. Cano, "A comparative performance evaluation of routing protocols for flying ad-hoc networks in real conditions," *Appl. Sci.*, vol. 11, no. 10, 2021.
- [4] Y. Ebazadeh and R. Fotohi, "A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold," *Secur. Priv.*, vol. 5, no. 1, 2022.
- [5] I. A. Abbasi, A. S. Khan, and S. Ali, "A Reliable Path Selection and Packet Forwarding Routing Protocol for Vehicular Ad hoc Networks," *Eurasip J. Wirel. Commun. Netw.*, vol. 2018, no. 1, 2018.
- [6] S. Thapar and S. K. Sharma, "Attacks and Security Issues of Mobile Ad Hoc Networks," *SSRN Electron. J.*, 2019.
- [7] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-Hoc networks: Evaluating the impact of attackers' strategies," *Sensors (Switzerland)*, vol. 18, no. 11, 2018.
- [8] M. A. Al-Shareeda and S. Manickam, "Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation," *Symmetry (Basel)*, vol. 14, no. 8, Aug. 2022.
- [9] J. Govindasamy and S. Punniakody, "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack," *J. Electr. Syst. Inf. Technol.*, vol. 5, no. 3, 2018.
- [10] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *J. Syst. Archit.*, vol. 105, 2020.
- [11] D. Hurley-Smith, J. Wetherall, and A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," *IEEE Trans. Mob. Comput.*, vol. 16, no. 10, 2017.
- [12] C. Borrego, M. Amadeo, A. Molinaro, and R. H. Jhaveri, "Privacy-Preserving Forwarding Using Homomorphic Encryption for Information-Centric Wireless Ad Hoc Networks," *IEEE Commun. Lett.*, vol.

23, no. 10, 2019.

[13] B. P. Kavin and S. Ganapathy, "A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves," *Int. Arab J. Inf. Technol.*, vol. 18, no. 2, 2021.

[14] M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, and A. S. Ahmed, "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021.

[15] M. Elhoseny and K. Shankar, "Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique," *IEEE Trans. Reliab.*, vol. 69, no. 3, 2020.

[16] T. H. Sureshbhai, M. Mahajan, and M. K. Rai, "An investigational analysis of DSDV, AODV and DSR routing protocols in mobile Ad Hoc networks," in *Proceedings - 2nd International Conference on Intelligent Circuits and Systems, ICICS 2018*, 2018.

[17] G. S. Ganpat Joshi, "A Novel Statistical Adhoc On-Demand Distance Vector Routing Protocol Technique is using for Preventing the Mobile Adhoc Network from Flooding Attack," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 6, 2021.

[18] P. Singh, M. Khari, and S. Vimal, "EESSMT: An Energy Efficient Hybrid Scheme for Securing Mobile Ad hoc Networks Using IoT," *Wirel. Pers. Commun.*, vol. 126, no. 3, 2022.