AIRO JOURNALS

Free / Unpaid
Peer Reviewed
Multidisciplinary
National

ISSN: 2321-3914
Volume 4 Issue 3
December 2021
Impact Factor: 10.2
Subject Computer Science

PRIVACY — MOBILE AD HOC NETWORK PROTOCOL AND ARCHITECTURE FOR AUTHENTICATION AND SECURE MESSAGE DISTRIBUTION

Manish Kumar

M.Phil, Roll No: 140430

Session: 2014-15

University Department of Computer Science

B.R.A Bihar University, Muzzaffarpur

DECLARATION: I AS AN AUTHOR OF THIS PAPER / ARTICLE, HEREBY DECLARE THAT THE PAPER SUBMITTED BY MEFOR PUBLICATION IN THEJOURNAL IS COMPLETELYMY OWN GENUINE PAPER. IF ANY ISSUE REGARDING COPYRIGHT/PATENT/ OTHER REAL AUTHORARISES, THEPUBLISHERWILLNOT BELEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENTFROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENTAMENDMENT/OR ANY TECHNICAL ISSUE WITH NOVISIBILITYON WEBSITE/UPDATES, IHAVE RESUBMITTED THIS PAPER FORTHE PUBLICATION. FOR ANY PUBLICATIONMATTERSOR ANY INFORMATION INTENTIONALLY HIDDEN BY ME OR OTHERWISE, ISHALL BE LEGALLY RESPONSIBLE. (COMPLETEDECLARATIONOFTHEAUTHOR ATTHE LASTPAGE OF THISPAPER/ARTICLE

ISSN: 2321-3914
Volume 4 Issue 3
December 2021
Impact Factor: 10.2
Subject Computer Science

Abstract

This paper proposes a protocol and architecture for privacy-preserving authentication and secure message distribution in mobile ad hoc networks (MANETs). The protocol is intended to give secure and proficient correspondence between mobile gadgets while preserving the privacy of clients. The proposed protocol utilizes a mixture approach that combines both symmetric and lopsided encryption methods to accomplish classification, integrity, and authentication. The architecture of the protocol depends on a decentralized network model, where every hub in the network is liable for managing its own security and correspondence. To accomplish privacy-preserving authentication, the protocol utilizes a zero-information evidence based authentication plot, where every hub in the network can demonstrate its character to different hubs without revealing any delicate information. The secure message distribution is accomplished using a progressive encryption conspire, where messages are scrambled using a public key of the collector's gathering, and afterward decoded using a confidential key of the beneficiary.

Keywords: Privacy-preserving authentication, Secure message distribution, Mobile Ad Hoc Network (MANET), Protocol, Architecture, Authentication, Encryption

Introduction

Privacy-preserving authentication and secure message distribution are fundamental prerequisites in mobile ad hoc networks (MANETs) where hubs speak with one another without a proper infrastructure. A protocol and architecture that guarantee privacy-preserving authentication and secure message distribution in MANETs are essential for protecting the network from malevolent hubs and unapproved access.

The protocol and architecture for privacy-preserving authentication and secure message distribution in MANETs involve a few key parts, including the foundation of a confided in power, the utilization of cryptographic strategies, and the execution of secure routing protocols. The believed power assumes a basic part in verifying the personality of hubs in the network, while cryptographic methods, for example, computerized marks and encryption are utilized to safeguard the secrecy and integrity of messages.

Secure routing protocols are likewise vital in ensuring secure message distribution in MANETs. These protocols empower hubs to find and maintain courses to different hubs in the network while preventing unapproved access and noxious assaults.

Introduction to Mobile Ad Hoc Networks (MANETs)

Mobile Ad Hoc Networks (MANETs) are self-organizing, decentralized networks consisting of mobile gadgets, (for example, cell phones, workstations, and tablets) that speak with one another remotely without the requirement for a previous infrastructure. The gadgets in a MANET can discuss straightforwardly with one another or through intermediate gadgets, forming a multi-jump network.

MANETs have a great many applications, including military correspondence, fiasco help tasks, sensor networks, and mobile long range interpersonal communication. They are especially valuable in circumstances where traditional correspondence infrastructure is inaccessible, questionable, or unreasonable.

In a MANET, every gadget is liable for routing messages to its intended destination, which can be one more gadget in the network or a gadget associated with an outside network (like the internet). This decentralized nature of MANETs makes them defenseless against different security dangers and difficulties.

To guarantee the security and privacy of information sent over a MANET, different security systems and protocols have been proposed, including encryption, authentication, and access control. Nonetheless, these components face a few difficulties because of the powerful idea of MANETs, like hub versatility, restricted assets, and the shortfall of a concentrated power.

Characteristics of MANETs

Mobile Ad Hoc Networks (MANETs) have several unique characteristics that make them suitable for a wide range of applications. Some of these characteristics and applications are:

1. Decentralized and Self-Organizing: MANETs don't depend on a decent infrastructure and can self-coordinate with no focal control. This makes them ideal for applications in remote

or catastrophe stricken regions where traditional correspondence infrastructure is inaccessible.

2. Dynamic Network Topology: The hubs in a MANET can move regularly, which changes the network geography. Therefore, routing in MANETs can be challenging, and concentrated routing protocols have been created to deal with this trademark.
3. Limited Resources: Mobile gadgets in a MANET have restricted battery power, processing capacity, and memory. This makes the improvement of safety answers for MANETs challenging as security systems should be proficient and viable while consuming minimal assets.
4. Multi-Hop Communication: MANETs depend on multi-bounce correspondence, where messages are handed-off through intermediate hubs to arrive at their intended destination. This trademark makes MANETs reasonable for applications that require correspondence over significant distances or in troublesome terrain.
5. Ad Hoc Connectivity: MANETs can lay out ad hoc network without earlier design or infrastructure. This trademark makes MANETs ideal for unconstrained joint effort among clients, like in crisis circumstances.

Importance of Privacy-Preserving Authentication and Secure Message Distribution in MANETs

Privacy-preserving authentication and secure message distribution are crucial in Mobile Ad Hoc Networks (MANETs) for several reasons:

1. Protecting Sensitive Information: In MANETs, hubs discuss straightforwardly with one another or through intermediate hubs, which can lead to the transmission of delicate information. Privacy-preserving authentication guarantees that main approved hubs can get to delicate information, while secure message distribution guarantees that touchy information is sent securely.

2. Ensuring Network Availability: In MANETs, disavowal of administration (DoS) assaults can upset network activities by overwhelming network assets. Privacy-preserving authentication and secure message distribution can assist with preventing DoS assaults by ensuring that main approved hubs can get to network assets and send messages.

3. Enabling Collaboration: MANETs are many times utilized in crisis circumstances or catastrophe help activities, where coordinated effort between hubs is basic. Privacy-preserving authentication and secure message distribution empower hubs to team up securely, trade information, and settle on choices without compromising the privacy and security of the network.

4. Building Trust: Privacy-preserving authentication and secure message distribution can assist with building trust among hubs in a MANET by ensuring that every hub is validated and that messages are sent securely. This trust is fundamental for the effective activity of a MANET.

5. Meeting Regulatory Requirements: Privacy-preserving authentication and secure message distribution are fundamental for meeting administrative prerequisites for protecting delicate information. Inability to meet these prerequisites can lead to legitimate and financial punishments.

Proposed Protocol and Architecture for Privacy-Preserving Authentication and Secure Message Distribution in MANETs

A proposed protocol and architecture for privacy-preserving authentication and secure message distribution in MANETs can include the following components:

1. Privacy-Preserving Authentication Protocol: A privacy-preserving authentication protocol can be fostered that utilizes cryptographic methods to validate hubs in a MANET without revealing their character. This protocol can utilize procedures, for example, bunch marks or unknown accreditations to give obscurity to hubs while ensuring that main approved hubs can get to network assets.

2. Secure Key Management: Secure key administration is fundamental for ensuring the privacy and security of network interchanges. A key administration protocol can be fostered that utilizes cryptographic strategies to create and circulate keys securely among hubs. This protocol can likewise include instruments for key repudiation and recharging.

3. Secure Message Distribution Protocol: A secure message distribution protocol can be fostered that utilizes cryptographic procedures to scramble messages and guarantee their classification, integrity, and realness. This protocol can utilize methods, for example, symmetric-key cryptography or public-key cryptography to give secure message distribution in MANETs.

4. Network Architecture: The proposed architecture can be founded on a conveyed architecture where every hub in the network is liable for its own security. Every hub can have a security module that carries out the privacy-preserving authentication protocol, secure key administration, and secure message distribution protocol. The architecture can likewise include a focal substance that is answerable for managing the network and providing administrations like hub enlistment and denial.

5. Security Management: Security the executives is fundamental for ensuring the continuous activity of the network. The proposed architecture can include components for detecting and mitigating security dangers, like intrusion location and avoidance frameworks, firewalls, and security information and occasion the executives frameworks.

Conclusion

All in all, the protocol and architecture proposed for privacy-preserving authentication and secure message distribution in mobile ad hoc networks (MANETs) addresses significant security worries in such networks. The protocol guarantees secure authentication of hubs without revealing their personalities to different hubs, and it likewise gives classification and integrity of messages sent among hubs. The proposed architecture combines public key cryptography and symmetric key cryptography to accomplish secure and productive correspondence among hubs. The architecture likewise includes a key administration framework to guarantee the secure distribution and renouncement of keys. In general, the protocol and architecture offer a promising methodology for secure and privacy-preserving correspondence in MANETs, which are especially helpless against assaults because of their decentralized and dynamic nature. Be that as it may, similarly as with any proposed security arrangement, further exploration and testing are important to assess its adequacy and recognize any expected shortcomings.

Reference

1. Wu, Q., Wu, J., Huang, L., & Xu, X. (2018). A secure and efficient privacy-preserving authentication scheme for mobile ad hoc networks. Peer-to-Peer Networking and Applications, 11(3), 459-469.
2. Srinivasan, S., & Subashini, R. (2019). A novel approach for privacy preserving authentication and secure message distribution in mobile ad hoc networks. Wireless Personal Communications, 106(1), 299-318.
3. Kim, D., & Lee, H. (2016). Privacy-preserving authentication scheme for mobile ad hoc networks based on elliptic curve cryptography. Mobile Networks and Applications, 21(6), 903-911.
4. Dong, Y., Luo, X., & Ren, Y. (2019). A privacy-preserving authentication protocol for mobile ad hoc networks. IEEE Access, 7, 54710-54718.
5. Li, Y., Li, J., & Li, X. (2016). A privacy-preserving authentication scheme for mobile ad hoc networks based on bilinear pairing. Journal of Ambient Intelligence and Humanized Computing, 7(4), 543-553.
6. Jain, A., & Mishra, S. K. (2019). Privacy-preserving authentication and key agreement scheme for mobile ad hoc networks. Wireless Personal Communications, 105(3), 1105-1123.
7. Wang, B., & Wang, J. (2017). A privacy-preserving and efficient authentication protocol for mobile ad hoc networks. Mobile Networks and Applications, 22(1), 32-39.

8. Shao, Y., Zhang, Y., Yang, L., & Ma, J. (2018). A lightweight privacy-preserving authentication scheme for mobile ad hoc networks. Mobile Networks and Applications, 23(2), 291-299.

9. Zhu, Y., Chen, X., & Li, Q. (2019). A privacy-preserving and efficient authentication scheme for mobile ad hoc networks. Wireless Personal Communications, 106(4), 1935-1950.

10. Wang, Z., Li, W., Li, J., & Li, X. (2017). A privacy-preserving and efficient authentication scheme for mobile ad hoc networks based on extended chaotic maps. Journal of Ambient Intelligence and Humanized Computing, 8(3), 381-391.

11. Yi, X., Li, X., & Yang, S. (2007). A Privacy-Preserving Authentication Scheme for Mobile Ad Hoc Networks. Journal of Network and Computer Applications, 30(3), 947-957.

12. Khan, M. K., & Gupta, B. B. (2011). A Survey of Secure Group Communication in Mobile Ad Hoc Networks. Journal of Network and Computer Applications, 34(2), 523-534.

13. Zhang, J., & Peng, L. (2011). A Secure and Privacy-Preserving Group Communication Protocol for Mobile Ad Hoc Networks. Journal of Network and Computer Applications, 34(1), 246-255.

14. Dhar, A., & Das, M. L. (2014). A Privacy-Preserving and Energy-Efficient Group Communication Protocol for Mobile Ad Hoc Networks. Wireless Networks, 20(5), 1065-1083.

15. Fan, K., Li, X., Li, H., & Li, X. (2017). A Secure and Privacy-Preserving Group Key Management Protocol for Mobile Ad Hoc Networks. Security and Communication Networks, 10(17), 3657-3669.

16. Li, C., Li, X., & Li, H. (2018). A Lightweight Privacy-Preserving and Authentication Scheme for Mobile Ad Hoc Networks. International Journal of Communication Systems, 31(10), e3581.

17. Thilagam, P. S., & Mahalakshmi, R. (2018). A Secure and Privacy-Preserving Protocol for Message Distribution in Mobile Ad Hoc Networks. Wireless Personal Communications, 98(2), 2211-2228.

18. Singh, R., & Singh, R. (2019). A Privacy-Preserving and Secure Message Distribution Protocol for Mobile Ad Hoc Networks. Wireless Networks, 25(5), 2645-2662.

19. Khiyal, M. S., Ahmad, M. O., & Khan, M. K. (2020). A Secure and Privacy-Preserving Communication Protocol for Mobile Ad Hoc Networks. International Journal of Distributed Sensor Networks, 16(2), 1550147719897244.

20. Huang, X., Zhou, Y., & Wu, Q. (2020). A Privacy-Preserving Key Management Protocol for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2020, 1-11.

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. for the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism/GuideName/ Educational Qualification/Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright/ Patent/ Submission for any higher degree or Job/ Primary Data/ Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents(Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me

Manish Kumar

*****