Lampyrid 2023: Volume 13, 524–530
ISSN: 2041-4900
https://lampyridjournal.com

Secure Message Transfer Using Pre-Existing Routing for Mantes

Mr. P. Prashanth Kumar[1], P. Navaneetha[2], B. Nagasri[3], D. Jashwini[4]
[1]Professor, Computer Science and Engineering, Sridevi Women's Engineering College Hyderabad, India
[2]Computer Science and Engineering, Sridevi Women's Engineering College, B. Tech IV Year Hyderabad, India
Email: [2]navaneethapatlolla123@gmail.com
[3]Computer Science and Engineering, Sridevi Women's Engineering College, B. Tech IV Year
Hyderabad, India
Email: [3]nagasri.bhagyala09@gmail.com
[4]Computer Science and Engineering, Sridevi Women's Engineering College, B. Tech IV Year Hyderabad, India
Email: [4]jashwinid726@gmail.com

Abstract
The rapid emergence and evolution of manet have made them popular in various use cases. Due to their flexibility and mobility, security protocols are being developed to protect these networks, but they only protect communication or routes, not both. For full protection we need to implement both secure routing and communication protocols. Hence to overcome these problems a secure framework secure message transfer using pre-existing routing for manet is proposed. it providing authentication to nodes , access can be control, and communication can be very secure.

Keywords: Authentication, routing, MANET

1. Introduction

Manets is a wireless network where node will communicate directly with each other without the need for infrastructure or centralized control. These networks are highly flexible and can be deployed in a variety of scenarios, from military operations to disaster relief efforts and beyond. Security is a major concern in MANETs due to their decentralized and distributed nature. Without the protection of a centralized infrastructure, nodes are vulnerable to a range of security threats, including eavesdropping, spoofing, and denial of service attacks. Therefore, secure communication in MANETs is of utmost importance for the success and reliability of these networks.

The Secure and Resilient Public Key Management for MANETs Secure message transfer using pre existing routing for mantes project is an ongoing research effort aimed at improving the security of MANETs through the development of a secure and perfect public key infrastructure (PKI). The project aims to provide a solution for secure communication in MANETs by enabling nodes to securely generate and exchange cryptographic keys without the need for a centralized authority. SUPERMAN is designed to be highly scalable, flexible, and resilient to various types of attacks, making it an ideal solution for MANETs in various scenarios.

2. Methodology

A. Secure message transfer using pre existing routing for mantes Architecture

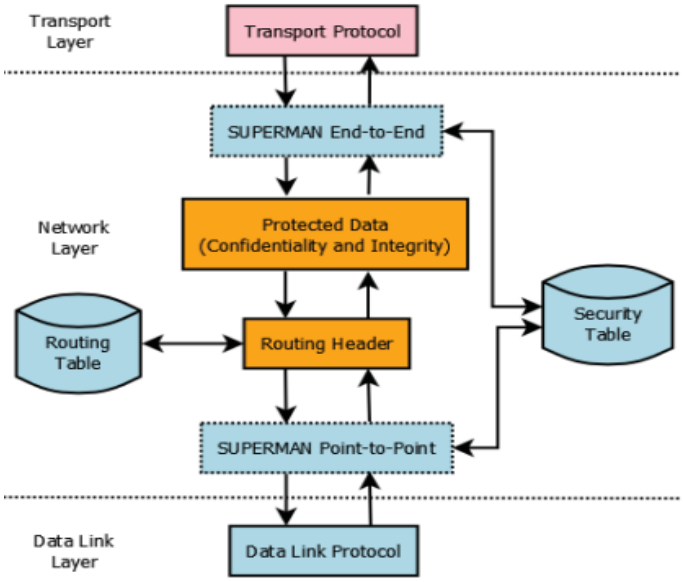

Figure 1.arcitecture of Secure message transfer using pre existing routing for mantes.

The OSI model's network layer, or layer 3, is where the UPERMAN architecture operates. It is made to give MANETs a completely secure communication infrastructure, without the need to change the routing protocol. The data flow is depicted in Fig. 1 from transport, to the network layer (which includes Secure message transfer using pre-existing routing for mantes.), to the data link layer. Elements Secure message transfer using pre existing routing for mantes that process packets and offer secrecy and integrity are shown by the dashed boxes. Additionally, Secure message transfer using pre existing routing for mantes. offers node authentication.

B. Implementation Details

Secure message transfer using existing routing for mantes.is a security mechanism designed for MANETs based on pre-existing routing protocols. It aims to provide

secure and efficient routing in MANETs without introducing additional routing overhead or modifying the existing protocols. In this , we communicate about the implementation details of Secure message transfer using pre existing routing for mantes. Key Management: Secure message transfer using pre existing routing for mantes., a centralized key management approach is used to generate and distribute keys. A Key Security Parameter (KSP) is generated by the centralized key distribution centre for each node in the network. The KSP includes a secret key, a key identifier, and other security-related parameters.

Authentication: To authenticate the nodes in the network, each node must have a unique identity that is verified by the other nodes. A node's identity is defined by its IP address, and a Certificate Authority (CA) is used to provide digital certificates that verify the identity of the node. Nodes generate a security association (SA) with each other after authentication.

Routing Protocol Integration:
Secure message transfer using existing routing for mantes. Integrates with existing routing protocols, like AODV and DSR (Dynamic Source Routing), to provide secure routing. Secure message transfer using existing routing modifies the routing protocol to use the SAs established between nodes for secure communication.

Packet Format:
Secure message transfer using existing routing for mantes.adds a security header to the existing packet format to indicate the type of security being used. The security header includes information such as the source IP address and destination IP addresses, the SA identifier, and the KSP identifier.

Summary:
Secure message transfer using pre existing routing for mantes.provides secure routing in MANETs without adding any extra overhead. It uses pre-existing routing protocols and a centralized key management approach for efficient key distribution. Authentication is done through digital certificates issued by a Certificate Authority, and SAs are established between nodes for secure communication. Finally, Secure message transfer using pre existing routing for mantes.changes the packet format by adding a security header to indicate the type of security used.

3. Results

There are multiple mathematical formulas that can be used to describe the security of MANETs using pre-existing routing protocols. One example is:
S = R * P

Where:

- S is the overall security level of the network
- R is reliability of the pre-existing routing protocol
- P is the effectiveness of the security mechanisms implemented on top of the routing protocol, like encryption, authentication, and intrusion detection.

The value of R can be calculated Based at the performance metrics of the routing protocol, like packet shipping ratio, delay, and overhead. The value of P may be calculated based totally on the electricity and performance of the security mechanisms used. Other mathematical formulas that can be used include entropy-based metrics for measuring randomness and unpredictability in the network traffic, and game-theoretical models for analysing the interactions between different nodes and the potential security threats they pose.

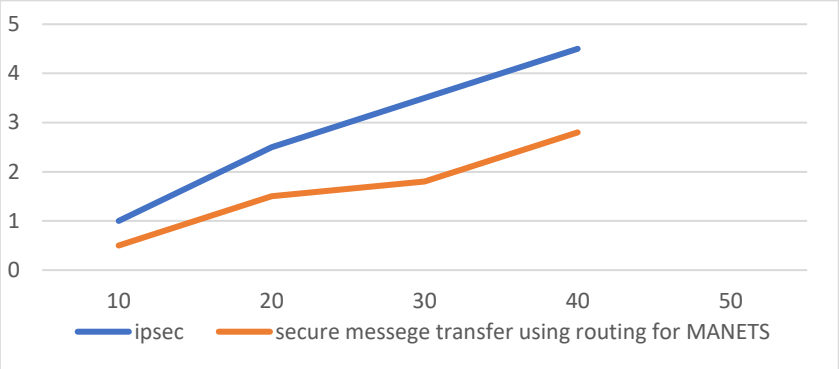

Fig 1 comparison between IPsec and secure massage transfer using routing for MANETS

Determines a analytical verbalization for the protection overhead of CBBA, under a likely safety foundation.

$$X=(f(c)*(d(d-1)))*(h+t)/k \qquad [1]$$

The f(x)is the someof rounds necessary by a likely harmony located distributed task distribution treasure.

The lot of knots is designated with d. The plunge and tag length (are depicted by h and t individually. It is pretended that the cargo of a bundle will be not surpass the Maximum Transmission Unit of the network connect. Hence, plunge and tag intensity is only considered late per bundle broadcast. Header proportion involves the IP plunge when taking everything in mind protocols which are not joined into the network stack (such as IPsec). The possibility of a bundle being brought is depicted apiece changeable k, that is fight the profit of 1 for this review, presumptuous no small deficit fully experiment stated on in this place paper. This equating holds valid for some non-clustered procedure of classifying tasks during the whole of a MANET. Equation (2) expands on the earlier proved (1), to detail in

what way or manner the safety overhead of a likely potocol maybe derivative for CF-CBBA task distribution.

$$Y=(\sum(1\leq i\leq l)\ 〚(x(i))〛)+x(k) \qquad [2]$$

The total count of bytes, y, is the produce of the total of all cluster distribution (depicted as instances of x). The changing k of x shows the cluster head distribution of CFCBBA, that is acted prior to aggressive the happening task lists to the cluster level for ending distribution with cluster appendages.

4. Conclusion

A cutting-edge security framework called secure message transfer using pre-existing routing for mantes. Guards the network securit and communication security in MANETs. Secure message transfer using pre-existing routing for MANTES

5. Reference

[1] P. S. Kiran, “Protocol architecture for mobile ad hoc networks,” 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.

[2] A. Chandra, “Ontology for manet security threats,” PROC. NCON, Krishnankoil, Tamil Nadu, pp. 171–17, 2005. 1536-1233 (c) 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See
http://www.ieee.org/publications_standards/publications/rights/index.html
for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2017.2649527, IEEE Transactions on Mobile Computing 14 IEEE TRANSACTIONS ON MOBILE COMPUTING, MANUSCRIPT ID

[3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, “A cluster-based approach to consensus based distributed task allocation,” in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.

[5] I. D. Chakeres and E. M. Belding-Royer, “Aodv routing protocol implementation design,” in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE, 2004, pp. 698–703.

[6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot et al., “Optimized link state routing protocol (olsr),” 2003.

[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, “Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, “Performance analysis of mesh routing protocols for uav swarming applications,” in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38– 47, 2004.

[10] N. Garg and R. Mahapatra, “Manet security issues,” IJCSNS, vol. 9, no. 8, p. 241, 2009.

[11] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, “An evaluation of protocols for uav science applications,” 2011.

[12] A. R. McGee, U. Chandrashekhar, and S. H. Richman, “Using itu-t x. 805 for comprehensive network security assessment and planning,” in Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International. IEEE, 2004, pp. 273–278.

[13] M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 3, pp. 106–107, 2002.

[14] F. Hong, L. Hong, and C. Fu, “Secure olsr,” in Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on, vol. 1. IEEE, 2005, pp. 713–718.

[15] A. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson, and Ø. Kure, “Secure extension to the olsr protocol,” in Proceedings of the OLSR Interop and Workshop, San Diego, 2004.

[16] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, “Dos attacks in mobile ad hoc networks: A survey,” in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012, pp. 535–541.

[17] S. Maity and S. K. Ghosh, “Enforcement of access control policy for mobile ad hoc networks,” in Proceedings of the Fifth International Conference on Security of Information and Networks. ACM, 2012, pp. 47–52.

[18] D. Hurley-Smith, J. Wetherall, and A. Adekunle, “Virtual closed networks: A secure approach to autonomous mobile ad hoc networks,” in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015, pp. 391–398.

[19] S. Bhattacharya and T. Basar, “Game-theoretic analysis of an aerial jamming attack on a uav communication network,” in American Control Conference (ACC), 2010. IEEE, 2010, pp. 818–823.

[20] S. Lu, L. Li, K.-Y. Lam, and L. Jia, “Saodv: a manet routing protocol that can withstand black hole attack,” in Computational Intelligence and Security, 2009. CIS’09. International Conference on, vol. 2. IEEE, 2009, pp. 421– 425.
[21] S. Zhao, R. Kent, and A. Aggarwal, “A key management and secure routing integrated framework for mobile ad-hoc networks,” Ad Hoc Networks, vol. 11, no. 3, pp. 1046–1061, 2013.
[22] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, “X. 509 internet public key infrastructure online certificate status protocol-ocsp,” RFC 2560, Tech. Rep., 1999.
[23] N. Doraswamy and D. Harkins, IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003.
[24] A. Ghosh, R. Talpade, M. Elaoud, and M. Bereschinsky, “Securing ad-hoc networks using ipsec,” in Military Communications Conference, 2005. MILCOM 2005. IEEE. IEEE, 2005, pp. 2948–2953.
[25] K. N. Ali, M. Basheeruddin, S. K. Moinuddin, and R. Lakkars, “Manipsec-ipsec in mobile ad-hoc networks,” in Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 1. IEEE, 2010, pp. 635–639.
[26] E. Rescorla, “Diffie-hellman key agreement method,” 1999.
[27] L. Harn, M. Mehta, and W.-J. Hsin, “Integrating diffiehellman key exchange into the digital signature algorithm (dsa),” Communications Letters, IEEE, vol. 8, no. 3, pp. 198–200, 2004.
[28] H. Krawczyk and P. Eronen, “Hmac-based extract and-expand key derivation function (hkdf),” 2010.
[29] A. Adekunle and S. Woodhead, “An aead cryptographic framework and tinyaead construct for secure wsn communication,” in Wireless Advanced (WiAd), 2012. IEEE, 2012, pp. 1–5.
[30] E. W. Dijkstra, “A note on two problems in connexion with graphs,” Numerische mathematik, vol. 1, no. 1, pp. 269–271, 1959.