International Journal of New Media Studies *ISSN: 2394-4331*
Vol. 4 Issue 2, July-Dec., 2017

A Survey on Trust Management Approaches for Secure Data Transmission in MANETs

Radhe Shayam Yadav

GBSE College, India

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are gaining traction due to their ability to spontaneously form wireless networks, independent of any fixed infrastructure. While these networks offer flexibility and self-configuration, ensuring secure data transmission and maintaining trust among participating nodes remains a challenge due to the dynamic nature of MANETs. This paper provides a comprehensive survey on existing trust management techniques that address the issue of secure data transmission in MANETs. We begin by outlining the fundamental characteristics of MANETs that present unique challenges, including frequent topology changes, limited resources, unreliable wireless connectivity, and the susceptibility to various security attacks. We then present a taxonomy of the trust management approaches in MANETs, which encompasses reputation-based systems, behavior-based systems, and cryptographic mechanism-based systems, offering a clear understanding of the mechanisms that underpin each approach.The paper delves into the intricate details of each trust management category, highlighting the critical aspects such as trust evaluation, trust propagation, attack resilience, and adaptability. We further analyze to provide a comparative evaluation of their suitability in various MANET environments and scenarios. In addition to this thorough investigation, we identify some trends and open challenges in trust management for secure data transmission in MANETs. We discuss potential research directions that may lead to the development of more resilient, adaptive, and scalable trust management solutions for future MANETs. By offering a systematic and in-depth analysis of existing trust management approaches, this survey contributes to a better understanding of the current state-of-the-art in MANET trust management research and provides researchers with insights for devising more efficient and effective methods to guarantee secure data transmission in highly dynamic networks.

Keywords: Trust Management, MANETS, cryptography, reputation based system, behaviour based system.

INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) have emerged as one of the most transformative communication technologies of the 21st century due to their spontaneous nature, adaptability, rapid deployment, and lack of reliance on fixed infrastructure. MANETs consist of a collection of highly dynamic and mobile devices connected through wireless links, enabling them to form impromptu wireless networks on-the-fly [1,2]. This characteristic makes them ideally suited for various applications such as disaster recovery, military operations, vehicular communications, and Internet of Things (IoT) deployments, among others [3,4].

However, the unique properties and characteristics of MANETs also pose several challenges, including ensuring secure data transmission and maintaining trust among participating nodes. Due to the unpredictable movement of devices, unstable wireless connections, limited resources, and absence of a centralized authority, MANETs are more susceptible to a range of security attacks, such as Sybil, blackhole, wormhole, and man-in-the-middle attacks, which can severely compromise data integrity and network performance [5-8].

Trust management serves as a vital component in addressing these challenges and assuring secure communications within MANETs. Trust management approaches aim to establish trust relationships among participating nodes, allowing them to make informed decisions about forwarding and processing data packets securely. A comprehensive understanding of the existing trust management approaches is crucial to addressing the ongoing vulnerabilities and developing advanced, resilient solutions for ensuring secure data transmission in MANETs [9].

This paper presents a comprehensive survey of the existing trust management approaches for secure data transmission in MANETs. We focus on reviewing the fundamental aspects of MANETs, including their characteristics, potential challenges, and security vulnerabilities, to underscore the need for robust trust management solutions. The main contribution of this paper is a systematic and in-depth analysis of the key trust management approaches, specifically reputation-based systems, behavior-based systems, and cryptographic mechanism-based systems, and their effectiveness in addressing the unique challenges

posed by the dynamic nature of MANETs. We critically assess the strengths and limitations of each approach to provide a comparative evaluation to aid researchers in devising innovative and improved methods for future research [10-13].

Additionally, this survey highlights open challenges, trends, and potential future research directions in trust management for secure data transmission in MANETs. The goal of this survey is to provide a thorough understanding of the current state-of-the-art in trust management research and serve as a foundation for enhancing secure data transmission in highly dynamic networks like MANETs [14].

Characteristics of Mobile Ad-hoc Networks (MANETs)

The fundamental characteristics of Mobile Ad-hoc Networks (MANETs) present unique challenges that stem from their dynamic and decentralized nature. These challenges include frequent topology changes, limited resources, unreliable wireless connectivity, and susceptibility to various security attacks, each of which can affect the network performance, stability, and overall security [15,16].

Frequent topology changes:

Nodes in a MANET have the ability to move freely, resulting in constantly changing network topologies. This fluidity complicates route establishment and maintenance, leading to increased control overhead and frequent route breaks, which negatively impact the stability, efficiency, and the overall performance of the network.

Limited resources:

MANET nodes often have constrained resources such as energy, processing power, storage, and bandwidth. These limitations can hinder network performance and scalability, requiring efficient routing and resource allocation protocols to optimize network stability and minimize the impact of resource constraints on data transmission [17,18].

Unreliable wireless connectivity:

Wireless communication in MANETs is characteristically unreliable due to factors including interference, multipath propagation, and fluctuating link qualities. This leads to an increased risk of packet loss, network partitioning, and unreliable data transmission, necessitating resilient communication and routing protocols to ensure reliable and efficient data delivery.

Susceptibility to various security attacks:

Due to the lack of central authority, MANET nodes rely on cooperation for efficient routing and data transmission, making them vulnerable to various security attacks. These attacks include passive eavesdropping, Sybil attacks, blackhole attacks, wormhole attacks, and man-in-the-middle attacks. Such attacks can compromise data integrity, confidentiality, and network performance, hence the importance of robust security measures and trust management mechanisms to protect the network and its participating nodes.

These unique challenges emphasize the need for advanced trust management approaches that can effectively ensure secure and reliable data transmission in MANETs, catering to their dynamic nature and other inherent constraints [18,19].

Taxonomy of the Trust Management Approaches in MANETs

Trust management approaches in Mobile Ad-hoc Networks (MANETs) are essential in maintaining the reliability and security of network communications. These approaches are generally classified into three primary categories: reputation-based systems, behavior-based systems, and cryptographic mechanism-based systems. Each of these categories serves different purposes and offers distinct benefits [20,21].

Reputation-based systems:

Reputation-based trust management systems work by evaluating the trustworthiness of nodes based on their past behavior and interactions with other nodes. These systems assign a reputation score that represents the trust level of a node. The process typically involves peers providing feedback on their experiences, helping to establish or modify the reputation scores of nodes they have dealt with. Properties such as cooperation, honesty, and reliability are factors in assessing a node's reputation [22-24].

Behavior-based systems:

These systems focus on directly observing and analyzing the actions and activities of network nodes. Behavior-based trust management systems can automatically detect and isolate malicious nodes that demonstrate irregular activity, such as data packet dropping or transmission errors. Direct observation of node behavior eliminates the possibility of false accusations or misreporting, resulting in a more reliable assessment of trustworthiness [25].

Cryptographic mechanism-based systems:

Cryptographic mechanism-based trust management systems use cryptographic techniques such as public-key cryptography, digital signatures, and certificates to establish secure communication channels and ensure data integrity within the network. These cryptographic tools enable nodes to authenticate each other's identities and verify the origin and authenticity of messages. Additionally, these systems ensure secure data transmission by providing end-to-end encryption.

Each of these three trust management approaches play a crucial role in maintaining the overall integrity,

security, and reliability of MANETs. A robust trust management scheme will often combine elements from each of these approaches to provide a comprehensive system that effectively addresses the challenges inherent in mobile ad-hoc networks [26,27].

Trust Evaluation, Trust Propagation, Attack Resilience, and Adaptability for Trust Management categories for MANETs.

Trust management in MANETs (Mobile Ad-hoc Networks) faces various challenges due to the network's dynamic topology, decentralized nature, and potential security threats. In order to effectively manage trust within these networks, it is necessary to consider four key concepts: trust evaluation, trust propagation, attack resilience, and adaptability [28,29].

Trust evaluation:

Trust evaluation is the process of assessing and determining the trustworthiness of network nodes. This is typically based on factors such as previous transactions, recommendations from other nodes, and observed behavior. Trust evaluation is essential for identifying trustworthy nodes and avoiding potential malicious activities. It plays a critical role in maintaining the security and integrity of network communication, particularly in terms of routing and data transmission.

Trust propagation:

Trust propagation refers to the dissemination of trust information among the nodes in the network. Efficient trust propagation is crucial for establishing and maintaining a reliable trust management system. This can be achieved by sharing information about the trustworthiness of individual nodes with other nodes throughout the network. Trust propagation helps nodes to make better decisions when choosing their neighbors and communication partners, based on trust levels and recommendations from others.

Attack resilience:

The potential for various types of attacks makes attack resilience an essential component of MANET trust management. Trust management systems need to identify, counter, and mitigate malicious activities, such as Sybil attacks, selfish behavior, or false reporting, that can compromise the security and proper functioning of the network. Attack resilience is critical in maintaining network reliability, as it ensures the identification and isolation of malicious nodes, preventing the spread of harmful activities.

Adaptability:

MANETs are characterized by dynamic topologies, with nodes continuously joining and leaving the network. As a result, trust management systems must exhibit adaptability to effectively address the changing network environments. Adaptive trust management systems can adjust trust evaluation criteria and methodologies, update trust ratings in real-time, and consider the evolving behavior patterns of nodes. Such adaptability enables trust management systems to remain effective and relevant, regardless of changes in the network's topology and structure.

By incorporating these four concepts into trust management systems, MANETs can achieve secure and reliable communication, enabling network nodes to make informed decisions about routing, data transmission, and interaction with fellow nodes [30-34].

Open Challenges in Trust Management for Secure Data Transmission in MANETs.

Trust management for secure data transmission in MANETs (Mobile Ad hoc Networks) is essential to ensure the integrity, confidentiality, and authenticity of information exchanged between nodes. Despite significant progress in this area, there are several open challenges that need to be addressed:

Dynamic topology: The constant changes in network topology due to the mobility of nodes make it difficult to maintain up-to-date routing information and trust relationships.

Scalability: As the number of nodes in the network increases, the task of managing trust relationships becomes increasingly complex. Developing lightweight and scalable trust management mechanisms is an ongoing challenge.

Limited resources: MANETs nodes typically have limited power, computation, and memory resources, which makes it difficult to implement resource-intensive cryptographic techniques and trust management algorithms.

Insider attacks: Vulnerability to malicious insiders makes trust management in MANETs challenging, as attackers could exploit node trust, thereby jeopardizing secure data transmission.

Trust evaluation metrics: Identifying and quantifying trust in a dynamic and varied context can be challenging. Developing accurate trust evaluation models that quickly adapt to changes in node behavior is an active area of study [33].

Lack of central authority: MANETs are decentralized networks without a central authority, which makes it difficult to implement traditional trust management techniques. Trust management approaches need to be distributed and self-organized to suit the decentralized nature of MANETs.

Reputation-based systems: Designing reputation-based systems to effectively evaluate the trustworthiness of nodes is an open challenge, as

factors such as signal attenuation, link breakage, and noise may lead to false trust evaluation.

Privacy preservation: Trust management mechanisms should protect the user's privacy. Balancing privacy needs with trust management requirements is an ongoing challenge.

Cooperation and incentives: Developing incentive mechanisms that encourage nodes to cooperate in trust management and share information without compromising their security is essential for robust MANETs [34].

Integrating heterogeneous networks: As MANETs become more heterogeneous, devising trust management mechanisms capable of interfacing with various network types and node capabilities remains an important open challenge.

Potential Research Directions that may lead to the Development of more Resilient, Adaptive, and Scalable Trust Management Solutions for Future MANETs.

There are several research directions that may lead to the development of more resilient, adaptive, and scalable trust management solutions for future Mobile Ad-hoc Networks (MANETs). Some of these promising research directions include:

Trust-based routing protocols: Develop trust-based routing protocols that integrate the concept of trust into the process of route selection, aiming to discover reliable and secure routes in the MANETs, and ensuring the authenticity and robustness of the entire network [35].

Machine Learning (ML) and Artificial Intelligence (AI) techniques: Utilize ML algorithms and AI techniques to process large amounts of real-time network data, and automatically adapt trust management mechanisms to various network conditions and potential attacks.

Blockchain technology integration: Incorporate blockchain technology into trust management in MANETs, enabling secure, transparent, and tamper-proof trust data recording, and efficient trust calculation and updates.

Lightweight and energy-efficient trust management: Implement lightweight and energy-efficient algorithms in the trust management system to optimize resource consumption and prolong the battery life of mobile nodes, while maintaining system resilience and trustworthiness.

Trust management strategies for IoT environments: Develop trust management solutions specifically tailored for IoT-based MANETs, due to their unique characteristics such as constrained devices and diverse communication modalities.

Cross-layer trust management: Investigate the impact of trust and security across different layers of the communication stack. Develop cross-layer trust management mechanisms that can synergistically enhance the overall trustworthiness, security, and resilience of MANETs.

Incorporating social network properties: Develop trust management models that incorporate social network properties in mobile nodes, such as recommendations, reputation, and similarity, to build a more realistic and better-trusted MANET environment [36].

Simulation and real-world testbeds: Conduct in-depth experiments and simulations in real-world environments to evaluate performance, scalability, adaptability, and resilience to potential attacks, while proposing improvements based on the results obtained.

Taking up any of these research directions has the potential to enhance and contribute significantly to the field of trust management in future MANETs [37-38].

CONCLUSION

In conclusion, the survey on Trust Management for Secure Data Transmission in MANETs reveals the growing importance and complexity of trust management solutions in protecting the integrity, confidentiality, and availability of data in Mobile Ad-hoc Networks. As the desire for enhanced communication in decentralized and dynamic environments continues to grow, the development of reliable and efficient trust management mechanisms becomes crucial. The reviewed literature demonstrates the rich history in this domain and highlights various trust management models and schemes, all driven by diverse objectives and different parameters.

The current focus is on creating trust management systems that strike a balance between resource consumption, scalability, adaptability, and resilience to ensure optimal network performance while maintaining security. Future research should explore innovative approaches such as machine learning, artificial intelligence, blockchain, and cross-layer trust management as they hold the key to fulfilling the evolving needs of MANETs and their applications. Novel trust management solutions must factor in the unique characteristics of IoT-based MANETs and the emerging significance of social network properties in determining trust relationships among mobile nodes.

The survey underscores the importance of continuous research, empirical evaluation in real-world scenarios, and the development of simulation models and

testbeds. These will help in maximizing the utility and effectiveness of trust management systems as well as providing insights into potential vulnerabilities and security issues facing MANETs. Overall, the pursuit of reliable and adaptive trust management solutions tailored specifically for MANETs plays a critical role in optimizing secure data transmission and fostering robust ad-hoc wireless networks for the future.

REFERENCES

[1]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.

[2]. Abate, A. F., Nappi, M., Riccio, D. and Sabatino, G., 2016. '2D and 3D face recognition: A survey', Pattern Recognition Letters, vol. 83, pp. 3-12.

[3]. Ahonen, T., Hadid, A. and Pietikainen, M., 2006. 'Face description with local binary patterns: Application to face recognition', Pattern Analysis and Machine Intelligence, IEEE Transactions, vol. 28, no. 12, pp. 2037-2041.

[4]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. IUP Journal of Computer Sciences, 4(3).

[5]. Allison, P. S. and Woodruff, M. E., 2014. 'Recognition of human iris patterns for biometric identification', Pattern Analysis and Machine Intelligence, vol. 33, pp. 116-119.

[6]. Arakala, A., Jeffers, J and Horadam, K., 2007. 'Fuzzy Extractors for Minutiae-Based Fingerprint Authentication', IEEE International Conference on Biometrics: Theory, Applications and Systems, Washington, DC, pp. 1-6.

[7]. Bengio, S. and Mariéthoz , J., 2004. 'A statistical significance test for person authentication', Proceedings of Odyssey 2004: The Speaker and Language Recognition Workshop, Toledo, Spain, pp 1-7.

[8]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In 2009 Second International Conference on Emerging Trends in Engineering & Technology (pp. 1143-1150). IEEE.

[9]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. International Journal of Computer Applications, 61(19).

[10]. Du, Y., Jiang, G. and Chen, P., 2009. 'Face recognition with radon transform and multilinear discriminant analysis', IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 23-34.

[11]. Fierrez, J., Ortega-Garcia, J., Ramos, D., and Gonzalez-Rodriguez, J., 2007. 'HMM-based on-line signature verification: Feature extraction and signature modeling', Pattern Recognition Letters, vol. 28, no. 16, pp. 2325-2334.

[12]. Hadid, A., Evans, N., Marcel, S. and Paalanen, P., 2004. 'Face analysis using local phase quantization', Proceedings of the 15th Scandinavian conference on Image analysis, Joensuu, Finland, pp. 737-745.

[13]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. J. Comput. Eng. Intel. Syst, 3(7), pp.32-41.

[14]. Jain, A.K., Hong, L. and Pankanti, S., 2000. 'Biometric identification', Communications of the ACM, vol. 43, no. 2, pp. 90-98.

[15]. Jain, A.K., Klare, B. and Park, U., 2015. 'Face matching and retrieval in forensics applications', IEEE MultiMedia, vol.2, no.1, pp.20–28.

[16]. Jobson, D.J., Rahman, Z., and Woodell, G.A., 1997. 'A multiscale retinex for bridging the gap between color images and the human observation

[17]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. International Journal Of Engineering Development And Research.

[18]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. International Journal of Computer Applications, 119(2).

[19]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. International Journal of Computer Applications, 116(19).

[20]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. International Journal on Computer Science and Engineering, 2(3).

[21]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. Recent Developments in Computing and Its Applications, p.155.

[22]. Bojan, J. and Pavešic, N., 2008. 'Face recognition using eigenfaces, Fisherfaces and support vector machines', Pattern Recognition, vol. 38, pp. 1788-1797.

[23]. Bowyer, K. W., Chang, K. and Flynn, P., 2016. 'A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition', Computer Vision and Image Understanding, vol. 101, no. 1, pp. 1-15.

[24]. Chen, Y., Dass, S.C., Jain, A.K., 2005. 'Fingerprint quality indices for predicting

authentication performance', AVBPA, vol. 3546, pp. 160-170.

[25]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11). International Journal of Computer Science & Communication, 1(1), pp.25-28.

[26]. Bhatnagar, D. and Rathore, R.S.,2015. CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES. International Journal of Advance Research in Science And Engineering, 4(01), pp.683-690.

[27]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. International Advanced Research Journal in Science, Engineering and Technology, 3(4), pp.83-86.

[28]. Crisan, D., Pana, S.C., Vasiu, R., 2015. 'Internet Security: A Case study of an integrated biometric authentication system', Procedia Technology, vol. 19, pp. 1016-1023.

[29]. Derawi, M.O., 2013. 'Accelerometer-Based Gait Analysis, A Survey', Biometrics Journal, vol. 7, no. 3, pp. 1-15.

[30]. Dessimoz, D., Richiardi, J., Champod, C. and Drygajlo, A., 2007. 'Multimodal biometric person authentication using distance-based classifier fusion', IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 37, no. 5, pp. 713-728.

[31]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. International Journal of Computer Applications, 138(8).

[32]. Mallick, A. S. B. and Rathore, R. K. Survey on Database Design for SaaS Cloud Application. International Journal of Computer Engineering and Technology, 6(6), 2015, pp. 64-71.

[33]. Ketki, S.K. and Rathore, M.R.S., 2015. A Novel Study for Summary/Attribute Based Bug Tracking Classification Using Latent Semantic Indexing and SVD in Data Mining. International Journal of Advanced Technology in Engineering and Science, 3(1), pp.214-220.

[34]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. International Journal on Computer Science and Engineering, 2(5), pp.1439-1444.

[35]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. IJCST, 6, pp.93-95.

[36]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. International Journal of Computer Applications, 1(13), pp.26-31.

[37]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. International Research Journal of Engineering and Technology (IRJET), 4(5), pp.153-155.

[38]. Dhillon, I. S., Prakash, S., and Sastry, P. S., 2007. 'A New Divide and Conquer Algorithm for VLSI Circuit Bi-Partitioning', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.