A survey of trust based secure routing protocol used in mobile ad hoc networks

Shalini Sharma[1], Syed Zeeshan Hussain[2]

[1]Department of Computer Science, Jamia Millia Islamia University New Delhi, India

[2]Department of Computer Science, Jamia Millia Islamia University New Delhi, India

Abstract. A mobile ad hoc network (MANET) is a dynamic wireless network developed using wireless nodes without using any infrastructures. The significant features of MANET are low-cost infrastructure, self-organization, mobility, and rapid deployment which offer the opportunity to deploy it for various applications such as disaster relief, environmental monitoring and military communications. The wireless nature of mobile networks causes the susceptible to malicious attacks. Therefore, security is turned out an essential factor to ease the secured message transmission among mobile nodes in the wireless medium. In this paper, the significant definition of the secure routing protocol is designated with its merits. Since there are various types of secure routing developed for accomplishing the secure transmission over the MANET. This paper studies the different types of existing routing methods such as optimization-based routing, and key encryption-based routing used in the MANET. The packet delivery ratio, energy consumption and end-to-end delay are considered key parameters for defining the effectiveness of secure routing protocols. This comprehensive research supports the researchers to obtain the best solutions for the current issues in the secure routing of MANET.

Keywords: Energy Consumption, Malicious Attacks, Mobile Ad Hoc Network, Packet Delivery Ratio, Secure Routing Protocol.

1. Introduction

MANET is a collection of mobile nodes that establishes communication without using the fixed physical infrastructure. MANET has different prominent characteristics such as rapid setup, varying topology, and multi-hop wireless communication. These characteristics make the MANET appropriate for numerous time-sensitive applications [1-2]. This ad hoc network provides a promising communication ability where the physical framework is tough to develop in the network. Additionally, the mobile nodes of MANET are used to transmit the data without using any administrative activities and physical framework [3]. The main difficulty of MANET is that the nodes have restricted energy resources where the nodes cannot be recharged in the network. The main objective is to provide a higher power-saving management approach in MANET. The clustering algorithm is developed to divide the nodes into various small groups where each cluster has one organizer node namely Cluster Head (CH) [4]. The constraints and eligibility are required to be summarized for deciding any node as CH. Here, the constraints are based on the information about node's residual power or energy [5]. The instability in power creates the CH to act erroneously and leads to formation of inefficient CHs which leads to node failure in MANET.

Routing protocols in MANET are used to discover the multi-hop route from the transmitter node to the receiver node. MANETs are a pre-established structure and self-configuring category of networks [6]. The incorporation of communication approaches and enhanced computing was used for expansion of ad-hoc networks. Numerous hardware and software architectures are developed with various applications; however, those architectures are failed to offer safety as it doesn't have firewalls and enough data security characteristics in ad hoc networks. The MANET is susceptible to various attacks from selfish to malicious nodes. Generally, the data transmission is mainly depending on each relay node, therefore securing the data communication is considered a significant problem [7]. Security development is important in various MANET applications such as vehicular applications, military applications, emergency operations and so on. This paper provides a study about different secure routing in the MANET. Moreover, this paper defines the advantages and disadvantages of various routing protocols.

The rest of the paper is arranged as follows: Section 2 provides the literature review of different secure routing developed in the MANET Section 3 provides the problem statement and in Section 4, the taxonomy of the survey is presented. Further, section 5 provides the comparative analysis and section 6 provides the discussion and analysis of this survey. Finally, the conclusion is presented in section 7.

2. Literature review

This section provides the literature survey about the different optimization trust-based routing protocols used in the MANET environment.

Mobile Ad-hoc Network is significant wireless, self-configuring, and structureless mobile network. However, due to changing nature of MANETs, secure transmission of data becomes the main problem of the network. Uppalapati Srilakshmi et al. [8] represented a multi path routing algorithm called Genetic Algorithm with the Hill Climbing technique which is used alternatively to traditional single-path data transmission. To minimize the fault tolerance and time consumption, the fuzzy C-means algorithm was used to determine the best cluster head for optimal route to packet distribution.

Mobile Ad-hoc Network is self-governing system that exchanges the effective data packet within the cellular area. Due to the poor system architecture, MANET is vulnerable to attacks and leads to loss of data packets which affects the overall efficiency of the network. Therefore, Neenavath Veeraiah et al. [9] introduced trust based cat slap single-player algorithm to effectively select the best routing. First, select the best cluster head using a fuzzy clustering algorithm based on direct, indirect, and recent trust. The C-SSA has integrated the merits of Salp Swarm Optimization and Cat Salp Optimization that are used to discover the route from the source to the destination. Therefore, the algorithm provides a tradeoff solution among both the mining and manipulation stages although, it was chosen only based on the trust values which doesn't support the performance of energy-efficient routing.

A collection of mobile nodes performs routing of packets and transmit the data effectively in MANET but the behavior of irrelevant nodes makes the main issues of the routing distribution. Ankita A. Mahamune and M. M. Chandane et al. [10] developed Ad hoc On-demand Distance Vector (AODV) routing protocol for the effective detection of malicious nodes. The AODV technique helps to interconnect the nodes to take part in effective communication. Moreover, it helps to diminish the irrelevant data and helps to attain better scalability with less memory storage to provide significant treatment to all interconnected nodes that participated in communication. However, the efficiency of the developed AODV was not suited for large-scale networks.

MANET is the collection of mobile nodes in wireless connectivity over the network. So due to the dynamic nature of the system, it requires static battery capacity because of the possibility of data loss. Therefore, R. Suganthi et al. [11] introduced a novel Trust efficient energy balanced Less Loss Routing Protocol (LLRP) for effective malicious node detection in MANET. The LLRP was used to improvise the network parameters by selecting the proper intermediate nodes. The parameters provide efficient computational for residual energy, the distance of the node, and the employed queue space of the node which helps to improve the routing of the system. Therefore, the protocol effectively selects the suitable path for sending the data to the base station.

MANET is one of the non-centralized, infrastructure-less, and self-organized wireless ad hoc networks used in the specific circumstances. Due to the network nature, it requires to secure source-to-destination connection. To ensure efficient communication, Moresh Madhukar Mukhedkar and Uttam Kolekar [12] represented Encryption Trust based Dolphin Glowworm Optimization for secure routing in MANET using advanced encryption standard -128. It obtained three parts namely; k-path discovery, best route selection, and communication thus selecting the optimal paths using the distance and trust value of nodes. The encryption standard used in this research ensures a secured path for routing even though there is less overhead in the network.

Limited resources in MANETs arises significant problems of network lifetime and data security. To select of the cluster head with minimal transmission overhead, Haseeb K and Islam N [7] represented Light Weight Secure and Energy-efficient Fog based Routing. The approach used two level of security using crypto graphs based secured keys. It improves the performance of the network with respect to energy consumption and network throughputs.

Ankita A. Mahamune and M. M. Chandane [13] have introduced trust based co-operative routing for secure communication in mobile ad hoc network. The trust scheme in proposed approach is validated by means of Evolutionary Self-Cooperative

Trust (ESCT) scheme, Generalized Trust Model (GTM), and the conventional AODV protocol. The proposed approach was highly scalable and known for its ability in detecting the malicious nodes with less computational complexity. However, the energy consumption was not considered while transmitting the data packets from source to destination.

Alagan Ramasamy Rajeswari et al [14] have introduced the soft computing based neuro fuzzy model which was based on Adaptive Network-based Fuzzy Inference System for Energy Efficient Secure clustering (ANFIS-EESC). Additionally, algorithms such as Weight-Based Trust Estimation (WBTE) and the Fuzzy-Based Clustering (FBC) were used to evaluate trustworthiness of the node and formation of clusters. The suggested approach elects the stable and trust aware nodes as CHs which aids in better network performance. But, the imbalance occurs while selecting the nodes with varying sizes.

3. Problem Statement

In this section, the design of secure routing in MANET includes many limitations while forwarding the data packets. Some of the open research problems that occurred in existing routing in MANET are defined as follows:

- The delay occurs while transmitting the data packets among the mobile nodes due to their battery incapability and destruction of mobile nodes [11-12]
- Data encryption is required to be developed for obtaining data privacy. Further, the malicious nodes are a risk to privacy, when the cryptographic keys aren't encoded and preserved in the node.
- In trust-based routing, the design of the protocol did not well work in the detection of the routing attacks thus will decrease the routing performance.
- Different methods are developed for secured data delivery from conventional mechanisms but still, they suffer from network overhead, insufficient security, unreliability, and decreased network throughput in the system.
- The local optima trap and network overfitting problem are increasing when a training user node is idle for data transmission.

4. Taxonomy of trust-based routing in MANETs

Security in MANET is an essential component for basic network functions like packet forwarding and routing. While considering the security in MANET, the trust levels between each node should be identified to detect the malicious nodes and determine the routing attacks of the system. During the route discovery process, a rogue node might readily provide false information because regular nodes opt to engage in node forwarding during the initial stages. It is necessary for addressing the security requirements in the MANET because the MANETs used in surveillance and combat functions-related applications where the sensors are required to process a large number of sensitive communications. The development of a secure and trust-based approach is required in MANET. Generally, various type of secure routing is developed to obtain reliable communication over the network. In this analysis, two different types of trust-based routing are examined to know their advantages and restrictions. The types of trust-based routing are mentioned as follows:

- Trust based routing using Optimization
- Trust based routing using Key encryption

The taxonomy of trust-based routing is shown in figure 1.

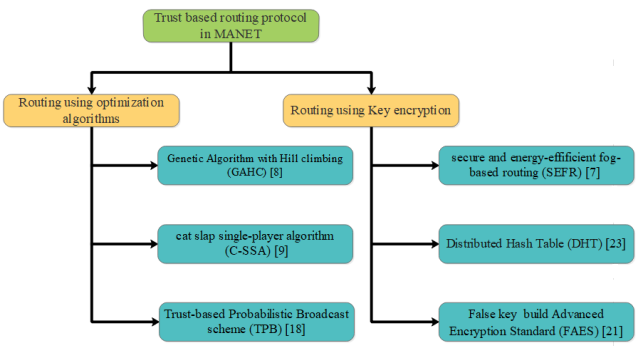

Figure 1. Taxonomy of trust-based routing algorithms

4.1 Routing using an Optimization algorithm

The examples for optimization algorithm-based routing involves Genetic Algorithm with Hill climbing (GAHC) [8], Cat Slap Single-Player Algorithm (C-SSA) [9], Trust Based Probabilistic Broadcast (TPB) scheme [16] and Trust Management System (TMS). The hybrid optimization approach is developed to identify the effective jumps in the MANET routing process [1]. The best route was determined by the overall cost being equal to the costs of the individual hops and thus will connect the link from the source node to the destination node. Examples of optimization algorithms are genetic algorithms with Hill Climbing Technology, Cat Slap Single Player, and Trust-based Probabilistic Broadcast, and so on. Additionally, Trust Management System (TMS) was developed which comprises data gathering, computation of trust level and trust-based establishment that performs interaction over each node for accomplishing reliable connections in the network. Figure 2 shows the architecture of TMS.

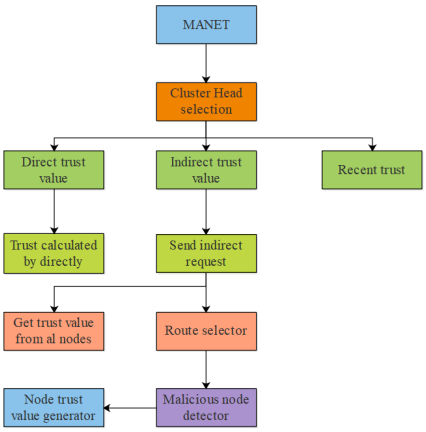

Figure 2. Architecture of TMS

CH selection applied with the maximum values of direct, indirect, and recent confidence to identify the malicious node, and then the intruded node was determined using the previous threshold node thus will enhance the best path of the secure data transmission from the source node to the destination. To rearrange the routing packets and identify the untrusted nodes from route discovery, the node's trust value and rebroadcast delay are determined. Additionally, the communication cost, residual energy, and data coverage should be considered in the secure transmission of data. The hybrid optimization approach effectively collects and transmits the data packets to the BS with secured communication.

4.2 Routing using Key Encryption

Some examples of methods which involves key encryption techniques for routing includes Secure and Energy-Efficient Fog based Routing (SEFR) [7], Distributed Hash Table (DHT) [21], False Key Build Advanced Encryption Standard (FAES) [19] and Ad Hoc On-Demand Multipath Distance Vector (AOMDV) [18]. The AOMDV is developed to identify the active transmission paths used to obtain secure data transmission. The multipath improvement of AOMDV is developed for improving the security against black hole attacks and secure data communication. The data is separated into various parts, once the path is discovered in the network. Subsequently, the false key build advanced encryption standard (FAES), Calculator Key, and Distributer Key scheme is used to encrypt each part of the data. At first, energy levels are assigned to each node in the network for the evaluation of utilizing residual activity levels, route discovery and route-critical nodes using Calculator Key and Distributer Key. Keys are generated by the CK node and sent to the DK. The created key pairs are delivered to the DK. In the communication, the source node's routing information is used to request the public key from the DK. Then DK delivers data to the routing database's encryption unit and send those data packets to the nearby nodes in the network. Moreover, the target node receives the data decryption key and helps to transmit the source node ID and helps the destination node to receive the data.

5. Comparative analysis

Numerous trust-based routing approaches are developed for MANET. Table 1 shows clear assessments of some significant contributions to the existing routing approaches.

Table 1. Comparative analysis

Author	Proposed methods	Advantages	Limitations	Performance measure
Deepika Kukreja et al. [15]	Effective detection and prevention of black/grey hole nodes using trust based energy and secure routing protocol in MANET. The intrusion detection technique was used to detect the malicious and hole nodes for the best route.	Less energy consumption as well as eliminates the misbehavior nodes and attacks effectively.	The energy consumption of the nodes was increased along with the increment in the node density.	Packet delivery ratio Packer drop ratio Control packet overhead End-to-end delay
Praveen Bondada et al [16]	A secure energy-efficient routing protocol was introduced using group key management. The group key management involves two specialized nodes such as Calculator Key (CK) and Distribution Key (DK) which helps to construct a secured key that provides secured transmission among the nodes.	The DK and CK nodes do not require to perform any extra calculations to generate the secret keys.	The developed key management considered trust and energy as primary factors to select the nodes. But distance is also required to be considered for developing an energy-efficient network	Packet delivery ratio End to end delay Energy consumption Throughput
Srinivas, M. and Patnaik, M.R [17]	The clustering and Secure Routing Protocol (SRP) were performed using a Quantum Worm Swarm Optimization (QGSO). The secure CHs were chosen using the QGSO which was optimized by using a trust factor, distance, energy and node degree. Subsequently, the Oppositional Gravitational Search Algorithm (OGSA) was used to perform the SRP in MANET.	The optimal route to the BS was discovered using the OGSA which was based on the opposition-based learning process.	However, the developed OGSA based SRP considered only distance as primary fitness.	End to end delay Energy consumption, Network lifetime Throughput.
Huaqiang Xu et al [18]	Trust-based Probabilistic Broadcast scheme (TPB) for minimizing the cluster overhead in malicious nodes. The lightweight trust management model was developed to rebroadcast computational for rearranging the routing packets to determine the best trust value of the system	The number of retransmissions was decreased in the TPB protocol for improving the data delivery.	The TPB mainly depends on the trust value and distance during the route discovery between the source and destination.	Packet delivery ratio Average rebroadcast ratio Normalized routing overhead End-to-end delay No. of CBR correction,
Mariappan Rajashanthi K. Valarmathi [19]	Secured multipath routing using Quality of Services for analyzing the trust value. The Ad hoc on-Demand Distance Vector-Backward Routing was applied to determine the trusted data packets. Homomorphic Encryption was used to encrypt the data for effective data distribution.	The developed AODV-based trusted routing was used to minimize the energy consumption	However, encryption was required to analyze a large-scale network.	Delay, detection rate Packet drop Throughput.
Yuma Shibasaki et al [20]	Represented Ad hoc on-demand Distance Vector (AODV) based routing protocol to achieve secure communication of nodes. The	The AODV effectively reduced the number of hops perform in the routing	The suggested AODV based routing protocol has limited computational ability	Hop count during route construction, Total byte during route construction

	Round Reply (RREP) was developed to initiate the reply to the intermediate node and helps to select an optimistic path to receive packets. Additionally, Raspberry Pi with C language was used to evaluate the time requirement of routing.	phase with minimum energy consumption.	which allows malicious nodes to get in and effects the secureness in routing	
Priyanka Singh et al [21]	Secure and reliable data transmission using Adhoc On-demand Multipath Distance Vector and K-Nearest Neighbor (KNN) for effective nearest node selection. Additionally, False key build Advanced Encryption Standard utilized to secure key encryption thus would enhance the secure connection with the least energy consumption.	This algorithm effectively used hardware implementation and to secure the protocol from black hole attacks in the system	However, the suggested approach provides poor transmission rate in complex networks of MANET	Energy consumption E2E delay Throughput
K. Karthick and R. Asokan [22]	Mobility aware routing protocol using hybrid optimization algorithm with QoS data transmission in MANETs. The animal migration optimization algorithm was developed for effective CH selection that was highly trustworthy and stable. Furthermore, enhanced ant colony optimization is used to select the best path among the source-destination for effective data transmission.	The MARP-HO algorithm helps to attain the state of energy efficiency during the transmission of data packets and helps to enhance the lifespan of the network.	High energy loss would be occurred due to a high amount of data transfer in the same node.	Delivery ratio Energy consumption Link stability Delay Loss ratio No. of dead nodes and Throughput Network lifetime

6. Discussion and analysis

This section describes about the overall discussion obtained while performing survey of various methodologies based on optimization based routing and key encryption based routing. The existing works based on optimization based routing methods such as clustering and Secure Routing Protocol (SRP) using a Quantum Worm Swarm Optimization (QGSO) [17] detect an optimal route to the BS based on the opposition-based learning process. The methodologies based on key encryption such as Ad hoc on-demand Distance Vector (AODV) based routing protocol [20] achieve secure communication of nodes by effectively reducing the number of hops perform in the routing phase with minimum energy consumption. In future, these fore mentioned drawbacks of the existing works can be considered and helps the researchers to introduce a secured routing protocol for an effective data transmission in MANET.

7. Conclusion

The secure routing protocol in MANET discovers the multi-hop secured path between source and destination nodes. A highly reliable secure route is significant for improving data delivery over the network. This paper offers the taxonomy of secure routing with its different types such as optimization-based routing, and key encryption-based routing used in the MANET. Various secure routing utilized in the MANET is examined with their advantages, and disadvantages along with their performance measures. This research is cooperative in identifying the modern trends in secure routing and its issues. Still, there is a huge amount of work is required to develop MANET for wireless applications. The state-of-the-art in the development of secure routing in MANET is known through this current analysis. This paper motivates researchers for many meaningful works.

References

[1] B.K. Tripathy, S.K. Jena, P. Bera, and S. Das, *An adaptive secure and efficient routing protocol for mobile ad hoc network,* Wireless Personal Communications, 114(2), pp.1339-1370, (2020)

[2] M.W. Kang, Y.W. Chung, *An improved hybrid routing protocol combining MANET and DTN*. Electronics, 9(3), p.439, (2020)

[3] M.S. Usha, K.C. Ravishankar, *Implementation of trust-based novel approach for security enhancements in MANETs*, SN Computer Science, *2*(4), pp.1-7, (2021)

[4] R. Ramalingam, R. Muniyan, A. Dumka, D.P. Singh, H.G. Mohamed, R. Singh, D. Anand, I.D. Noya, *Routing Protocol for MANET Based on QoS-Aware Service Composition with Dynamic Secured Broker Selection*, Electronics, 11(17), p.263, (2022)

[5] N. Panda, B.K. Pattanayak, *ACO-based secure routing protocols in MANETs,* In New Paradigm in Decision Science and Management (pp. 195-206). Springer, Singapore (2020)

[6]. K.V. Kumar, T. Jayasankar, V. Eswaramoorthy, V. Nivedhitha, *SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks*, International Journal of Intelligent Networks, 1, pp.36-42 (2020)

[7] K. Haseeb, N. Islam, Y. Javed, U. Tariq, *A lightweight secure and energy-efficient fog-based routing protocol for constraint sensors network,* Energies, 14(1), p.89 (2020)

[8] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S.A. Alghamdi, O.I. Khalaf, B.V. Subbayamma, *An improved hybrid secure multipath routing protocol for MANET*, IEEE Access, 9, pp.163043-163053 (2021)

[9] N. Veeraiah, O.I. Khalaf, C.V.P.R. Prasad, Y. Alotaibi, A. Alsufyani, S.A. Alghamdi, N. Alsufyani, *Trust aware secure energy efficient hybrid protocol for manet.* IEEE Access, 9, pp.120996-121005 (2021)

[10] A.A. Mahamune, M.M. Chandane, *Assn Efficient Trust-Based Routing Scheme Against Malicious Communication in MANET*, International Journal of Wireless Information Networks, 28(3), pp.344-361 (2021)

[11] R. Suganthi, I. Poonguzhali, J. Navarajan, R. Krishnaveni, N.N. Saranya, *Trust based efficient routing (TER) protocol for MANETS*, Materials Today: Proceedings (2021)

[12] M.M. Mukhedkar, U. Kolekar*, E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network*, International Journal of Communication Systems, 33(7), p.e4252 (2020)

[13] Mahamune, A. Ankita, and M. M. Chandane. *Trust-based co-operative routing for secure communication in mobile ad hoc networks,* Digital Communications and Networks (2023).

[14] A.R. Rajeswari, W.C. Lai, C. Kavitha, P.K. Balasubramanian, and S.R. Srividhya, *A Trust-Based Secure Neuro Fuzzy Clustering Technique for Mobile Ad Hoc Networks*, Electronics, 12(2), p.274 (2023)

[15] D. Kukreja, D.K. Sharma, *T-SEA: trust based secure and energy aware routing protocol for mobile ad hoc networks*, International Journal of Information Technology, 14(2), pp.915-929 (2022)

[16] P. Bondada, D. Samanta, M. Kaur, H.N. Lee, *Data security-based routing in MANETs using key management mechanism*, Applied Sciences, 12(3), p.1041 (2022)

[17] M. Srinivas, M.R. Patnaik, *Clustering with a high-performance secure routing protocol for mobile ad hoc networks*, The Journal of Supercomputing, 78(6), pp.8830-8851 (2022)

[18] H. Xu, H. Si, H. Zhang, L. Zhang, Y. Leng, J. Wang, D. Li, *Trust-based probabilistic broadcast scheme for mobile ad hoc networks*, IEEE Access, 8, pp.21380-21392 (2020)

[19] M. Rajashanthi, K. Valarmathi, *A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs,* Wireless Personal Communications, 112(1), pp.75-90 (2020)

[20] Y. Shibasaki, K. Iwamura, K. Sato, *A Communication-Efficient Secure Routing Protocol for IoT Networks, Sensors,* 22(19), p.7503 (2022)

[21] P. Singh, M. Khari, S. Vimal, *EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT*, Wireless Personal Communications, 126(3), pp.2149-2173 (2022)

[22] K. Karthick, R. Asokan, *Mobility aware quality enhanced cluster based routing protocol for mobile ad-hoc networks using hybrid optimization algorithm,* Wireless Personal Communications, 119(4), pp.3063-3087 (2021)

[23] Kousar, R., Alhaisoni, M., Akhtar, S.A., Shah, N., Qamar, A. and Karim, A., *A secure data dissemination in a DHT-based routing paradigm for wireless ad hoc network,* Wireless Communications and Mobile Computing, 2020, pp.1-32 (2020)