International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 52, No. 3, June, 2019, pp. 253-256
Journal homepage: http://iieta.org/journals/jesa

Secure Data Transmission with Effective Routing Method Using Group Key Management Techniques-A Survey

Rajesh Yamparala[1,2*], Balamurugan Perumal[1]

[1] Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, Tamil Nadu, India
[2] Department of CSE, Vignan's Nirula Institute of Technology & Science for Women, Guntur, Andhra Pradesh 522005, India

Corresponding Author Email: rajeshyamparala@gmail.com

https://doi.org/10.18280/jesa.520305

Received: 12 March 2019
Accepted: 28 May 2019

Keywords:
mobile ad hoc networks, secure data transmission, routing methods, key management techniques

ABSTRACT

Mobile Ad hoc Networks (MANETs) are a subclass of remote network system having exceptional characteristics of dynamic system topology and moving nodes. The utilization of remote advances is expanding and it impacts in the improvement of new hypotheses and structures for the interchanges. One of these new advancements is the portable systems. The routing is a fundamental part in the achievement of the secure communication in these structures. Routing method is the basic and essential execution factor in the Mobile Ad-hoc Network. The routing methods in MANET are practiced to deal with much number of nodes with limited resources. There is an assortment of routing method exist in MANET. Because of the dynamic topology and non-framework, network members collaborate with their neighbors to route the data packets. Cryptographic methodologies have been familiar with secure gathering for example, Private and Public Key Infrastructure. The self-governing and circulated nature of MANETs requests a decentralized validation administration, where Public Key Infrastructure is viewed as a superior arrangement. Key administration in the MANET is a critical issue concerning the security of the network communication. By setting up key administration technique, arrangement can be given to administrations like confirmation, information respectability and information classification. Secure routing and information transmission have an important role in Ad Hoc system as it is increasingly defenseless against numerous attacks because of its auxiliary qualities. In this paper, a survey is done on different routing methods, secure communication process and methods to improve the unwavering quality of information transmission.

1. INTRODUCTION

The qualities of the Ubiquitous Computing, thought by Weiser [1], have been impacting the improvement and the utilization of remote advancements. The ad hoc network structures can be utilized in circumstances where a wired system can't, chiefly in conditions where it is not possible to establish the fixed network [2]. The MANETs are one of the expansions of the remote advancements. The MANETs are not infra-organized. They have no control in charge of the system's administration. These systems are called specially appointed as a result of their dynamic structure [3]. The network may have portable nodes (MANETs – Mobile Ad-hoc Networks). In a MANET the nodes move randomly with various directions. The absence of a brought together control in these structures, the nodes versatility and the dynamic topology enable numerous relevance situations to the MANETs [4].

1.1 Routing protocol types

There are distinctive routing methods existing in MANET. Routing methods can be characterized into three types: Proactive, Reactive routing method and Hybrid methods. The routing methods in MANET are practiced to deal with significantly number of nodes with limited resources [5]. The real worry in routing method is entering/leaving of the nodes in network [6]. It is essential to reduce routing message overhead in spite of the developing number of portable nodes. Another essential concern is to keep up the measure of routing table little provided that the extent of routing method is bigger than it can influence the control packets exchanged inside the system [7]. Routing method is arranged on how and at what time routes are found, the shortest route to the destination is chosen.

Proactive Routing Protocols

This sort of routing methods utilizes interface state routing calculations which floods connected data about its neighbors as often as possible. Proactive routing method stores the routing data and keeps up the data update. The instances of proactive routing methods are DSDV, OLSR, and WRP etc.

Reactive Routing Protocols

Reactive routing methods try to reduce overheads that are available in proactive methods. It utilizes demand vector routing calculation and builds up the route to given reciever just when a node demand it by starting route revelation process [8]. There are number of Reactive routing methods accessible in MANET4 like DSR, AODV, TORA and LMR and so forth.

Hybrid Routing Protocols

It is the combination of Reactive and proactive routing methods. The case of Hybrid routing methods are ZRP, BGP, EIGRP [9]. Figure-1 illustrates the Proactive, Reactive routing method and Hybrid methods.

The figure 1 demonstrates the case of the kind of routing method.

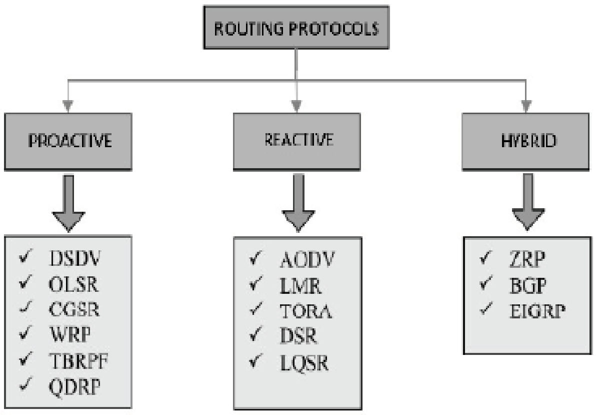

Figure 1. Routing protocols

MANETs comprises of portable specialized gadgets, for example, workstations, cell phones and individual computerized associates. Rather than utilizing a brought together routing administration, cell phones collaborate with one another to forward data from source to destination in a multi-jump way [10]. There is no framework in MANETs, every client just knows his neighbors next step to it. There are a few central contrasts between wireless and wired systems:

(a) Dynamic Topology: Network terminals can move unreservedly at certain speed, consequently arrange topology is continually changing and scarcely to be anticipated;

(b) Resource Requirements: Mobile terminals can be notepads, PDAs or cell phones [11]. They all have restricted calculation power and short battery life;

(c) No Framework: Ad hoc system is intended to be conveyed quickly. Versatile clients participate to route parcels, and along these lines there is no need of incorporated administrations; and

(d) Limited Physical Security: Mobile gadgets, for example, note pads, PDAs and cell phones don't have solid secure frameworks because of expense and constrained power [12]. The convenience and steady quality of portable networks emphatically relies upon its security. Be that as it may, because of its transparency and absence of brought together administrations, giving a protected domain is as yet a difficult undertaking for a portable networks. It is difficult to accomplish classification and credibility in such system [13].

There are various diverse attacks that objective the portable networks, running from easy to refined ones. For instance, an attacker can involve in data gathering of other nodes or just disposing of information it receives. Malicious routing attacks can disturb routing revelation or support the standards characterized by the routing methods. Progressively complex attackss incorporates blackhole [14], byzantine [15], wormhole [4] and many more.

Cryptographic methods have been brought into MANETs to verify data interchanges. These incorporates Private and Public Key Infrastructure. Private Key Infrastructure enables at least two clients to set up secure communication by sharing a typical secret key. In any case, in a system with quantities of clients, such key understanding method requires substantial message exchage [16]. Public Key Infrastructure utilizes a couple of keys to encode/decode messages. Private key is stayed quiet while public key can be generally appropriated. It decreases the message trading overhead as in Private Key Infrastructure. Along these lines key validation administration ought to likewise be decentralized and self-sufficient.

1.2 Security challenges overview

Security attacks:

While MANETs can be rapidly and reasonably setup as required, security is an increasingly basic issue contrasted with wired systems or different remote partners. Numerous uninvolved and dynamic security attacks could be propelled from the outside by malicious hosts or from within by traded off hosts [17].

Passive attacks:

In latent attacks, an intruder catches the information without adjusting it. The attacker does not change the information and does not infuse extra traffic. The objective of the attacker is to acquire data that is being transmitted, in this way abusing the message secrecy. Since the action of the system isn't upset, these attacks are hard to identify [18]. An encryption system can lighten these attacks, making it hard to peruse the transmitted information.

Active attacks:

In dynamic attacks, an attacker effectively takes part in disturbing the typical task of the system administrations. An attacker can make a functioning attack by altering packets or by presenting false data. Dynamic attacks can be additionally partitioned into inside and outer attacks: interior attacks are from traded off nodes that were at one time a real piece of the system. Since the opponent is now part of the system as approved nodes, they are significantly more serious [19] and hard to distinguish contrasted with outside attacks. Outer attacks are conveyed by nodes that are not a real piece of the system. Such attacks are frequently anticipated through firewalls or some verification and encryption components.

Security issues and their present arrangements in the portable networks were examined [20]. With the powerless idea of the versatile networks, there are various security dangers that wind up its improvement. At long last the present security solutions for the MANETs are analyzed in this manuscript.

2. LITERATURE SURVEY

Sumathi et al. [1] proposed a group based adaptable key administration method for Ad hoc systems. Their proposed method is identified with another grouping method. The system is isolated into networks or groups dependent on liking connections between nodes. So as to ensure the interchanges between nodes they proposed two sorts of keys produced by each cluster head. The method is versatile as per the limitation of the portable nodes, battery control and to the dynamic system topology changes. This proposed methodology of clustering is based versatile key administration method that gave ensured communications between the nodes of the Ad hoc systems.

A key administration proposition for secure communication in MANETs was depicted by Kuo et al. [2]. They show a various leveled key administration technique for secure gathering communications in MANETs. For security, they scrambled a packet twice. They additionally speak about gathering upkeep in their paper so as to manage changes in the topology of a MANET. Finally, they did an act examination to contrast their proposed plan and other customary techniques that are utilized for key administration in MANETs. The outcomes show that their proposed strategy performed well in giving secure communication in MANETs.

Hinge et al. [3] proposed a technique for key administration that gives excess and power to Security Association (SA) foundation between sets of nodes in MANETs. They have worn a changed progressive trust Public Key Infrastructure (PKI), which nodes can definitely expect the executives jobs. Moreover they utilized non-revocation through a progression of communication and checks to safely impart new nodes data among Certificate Authorities (CAs). They inferred that nodes could leave and join the system whenever required. Nodes could produce their very own cryptographic keys and were capable of protecting communication with different nodes. So as to balance the adaptability and expanded accessibility of the Key Management Scheme (KMS), security was given by acquainting two ideas likewise with disavowal and security cautions: non-revocation and conduct reviewing. The KMS decided adequate dimensions of security by joining node confirmation with an extra component, node conduct. A conduct reviewing plan is fundamental every node to review the conduct of different nodes.

Another key administration method for remote communication was expressed by Venkanna et al. [4]. They set forth an efficient gathering key dispersion method which depends on multi-party Diffie-Hellman key exchange and which is likewise password authenticated. The essential thought of the method is to safely develop and convey a secure session key, 'K,' among a gathering of nodes/clients who need to impart among themselves in a protected way. The secret word 'P' is additionally most basic among each legitimate part present in the situation. This 'P' helps for verification process and anticipates man in-the-middle attack. In contrast to a few different methods, the proposed methodology does not require communicate/multicast ability.

Malathi et al. [5] proposed group based security design for Ad hoc systems. They proposed and unsurprising security idea dependent on a disseminated confirmation. A system is partitioned into groups with one novel head node for each cluster. These cluster head nodes do authoritative capacities and offers a system key among different individuals from the group. In addition a similar key is utilized for affirmation.

The key administration in the appropriated methodology is accomplished by all the multicast network individuals, which participate and work together to guarantee a multicast secure communications between them, which suggests that methods having a place with this methodology don't scale. Inside this methodology, Singal, et al. [7] propose a circulated key administration method for MANETs, in view of the GPS measures and on the gathering key trade protocol GDH (Group Diffie Helmann).

At method instatement, every node in the specially appointed system, floods its GPS data and its public key to all the others nodes, creating a costly overhead of energy and transfer speed utilization. Utilizing the GPS data considered from others nodes, each gathering part can build the system topology. The source of the cluster multicasts to all the cluster individuals the gathering key, processed as a development of their public keys, as indicated by the multicast tree built up [5]. The decentralized methodology creates the multicast group into sub-gatherings, each sub-cluster is overseen by a neighborhood controller in charge of the security the executives of the individuals from its sub-gathering. We recognize two sorts of decentralized methods: static grouping and dynamic bunching methods.

Watch dog method neglects to identify malicious misbehaviors. TWOACK is proposed as for the six shortcomings of the Watchdog method. The TWOACK plan effectively tackles the restricted transmission power and recipient impact issues. Because of the constrained battery control nature of MANETs, such excess transmission procedure can without much of a stretch debase the life expectancy of the whole system.

Jhaveri et al. [8] presents a Source Driven Self selection (SDSS) calculation dependent on versatility for the route disclosure process. In this calculation, the source node is essentially mindful which indicates the required utility measurement in each RREQ packet. The source node starts by figuring the portability utility capacity. It primarily builds the dependability of the route over visually impaired transmission and it likewise lessens the communication issue because of less rebroadcasting modes amid route disclosure.

3. PROPOSED METHODOLOGIES

Based on the above problems identified in route identification, key generation and key maintenance and secure data transmission there is a necessity for achieving the following.

- ➢ To develop a powerful routing technique which gives QoS based security to multicast routing in MANET.
- ➢ To design a powerful key administration procedure which will generate and maintain multi key structures in MANET.
- ➢ To develop a technique for packet loss reduction to enhance the productivity of the network there by decreasing the expense and overhead.
- ➢ To develop an algorithm for reducing the overall overhead of the network.

4. CONCLUSION

In this manuscript different issues related with Ad Hoc systems, especially more issues in Routing on Ad Hoc system, group key management and secure data transmission issues are studied. In planning any safety efforts for MANETs, it is expected to think about different qualities of attack. A noteworthy risk to the security in MANETs is Packet-dropping attack. To build the benefits of the current framework we proposed Hybrid cryptography. In half breed system, the nodes can arrange the session key for secure communication that satisfies the necessity of Authentication. Security communication demonstrate that the proposed method builds up a secure route from various sort of attacks. We examined these methods and new methodologies need to be proposed for overcoming the issues in routing, group key management and secure data transmission.

REFERENCES

[1] Sumathi, K., Priyadharshini, A. (2015). Energy ptimization in MANETs using on-demand routing

protocol. Procedia Comput. Sci., 47: 460-470. https://doi.org/10.1016/j.procs.2015.03.230

[2] Kuo, W.K., Chu, S.H. (2016). Energy efficiency optimization for mobile Ad Hoc networks. IEEE Access, 4: 928-940. https://doi.org/10.1109/access.2016.2538269

[3] Hinge, R., Dubey, J. (2016). Opinion based trusted AODV routing protocol for MANET. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS), Udaipur, India, 4-5. ACM: New York, NY, USA, 2016. https://doi.org/10.1145/2905055.2905342

[4] Venkanna, U., Agarwal, J.K., Velusamy, R.L. (2015). Cooperative routing for MANET based on distributed trust and energy management. Wirel. Pers. Commun., 81: 961-979. https://doi.org/10.1007/s11277-014-2165-5

[5] Malathi, M., Jayashri, S. (2016). Robust against route failure using power proficient reliable routing in MANET. Alexandria Engineering Journal, 57(1): 11-21. https://doi.org/10.1016/j.aej.2016.10.004

[6] Chavhan, S., Venkataram, P. (2015). Emergent intelligence based QoS routing in MANET. Procedia Comput. Sci., 52: 659-664. https://doi.org/10.1016/j.procs.2015.05.068

[7] Singal, G., Laxmi, V., Gaur, M.S., Todi, S., Rao, V., Tripathi, M., Kushwaha, R. (2017). Multi-constraints link stable multicast routing protocol in MANETs. Ad Hoc Netw., 63: 115-128. https://doi.org/10.1016/j.adhoc.2017.05.007

[8] Jhaveri, R.H., Patel, N.M. (2017). Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. IJCS, 30. https://doi.org/10.1002/dac.3148

[9] Sarkar, S., Datta, R. (2016). A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Ad Hoc Netw., 37: 209-227. https://doi.org/10.1016/j.adhoc.2015.08.020

[10] Sirisala, N., Bindu, C.S. (2016). A novel QoS trust computation in MANETs using fuzzy petri nets. Int. J. Intell. Eng. Syst., 10: 116-125. https://doi.org/10.22266/ijies2017.0430.13

[11] Khamayseh, Y.M., Aljawarneh, S.A., Asaad, A.E. (2017). Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. Sustainable Computing: Informatics and Systems, 18: 90-100. https://doi.org/10.1016/j.suscom.2017.07.001

[12] Sethuraman, P., Kannan, N. (2017). Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wirel. Netw., 23: 2227-2237. https://doi.org/10.1007/s11276-016-1284-1

[13] Ahmed, M.N., Abdullah, A.H., Chizari, H., Kaiwartya, O. (2017). Flooding factor based trust management framework for secure data transmission in MANETs. J. King Saud Univ. Comput. Inf. Sci., 29: 269-280. https://doi.org/10.1016/j.jksuci.2016.03.004

[14] Kambourakis, G., Konstantinou, E., Douma, A., Anagnostopoulos, M., Fotiadis, G. (2010). Efficient certification path discovery for MANET. EURASIP. J. Wirel. Commun. Netw., 243985. https://doi.org/10.1155/2010/243985

[15] Narayana, V.L. (2018). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs. Smart Innovation, Systems and Technologies, 649-658. https://doi.org/10.1007/978-981-13-1921-1_63

[16] Rajkumar, B., Narsimha, G. (2016). Trust based certificate revocation for secure routing in MANET. Procedia Comput. Sci., 92: 431-441. https://doi.org/10.1016/j.procs.2016.07.334

[17] Cho, J.H., Chen, I.R., Kevin, S.J. (2016). Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Netw., 44: 58-75. https://doi.org/10.1016/j.adhoc.2016.02.014

[18] Papadimitratos, P., Haas, Z.J. (2003). Secure link state routing for mobile ad hoc networks. In Proc. IEEE CS Workshop on Security and Assurance in ad hoc Netw., Orlando, FL, pp. 379-383. https://doi.org/10.1109/saintw.2003.1210190

[19] Hu, Y., Perrig, A., Johnson, D.B. (2003). Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1): 175-190. https://doi.org/10.1016/s1570-8705(03)00019-2

[20] Gopi, A.P., Narayana, V.L. (2018). Dynamic load balancing for client server assignment in distributed system using genetical algorithm. Networking and Information Systems ARTICLE, 23(6): 87-98. https://doi.org/10.3166/isi.23.6.87-98