Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.S1, 2018, pp.20-23

DOI: https://doi.org/10.51983/ajcst-2018.7.S1.1812

Routing Methods in MANET with Secured Key Management and Packet Drop Reductions: A Survey

Yaswanth Kumar Alapati[1] and Suban Ravichandran[2]
[1]Research Scholar,[2]Assistant Professor
[1&2]Department of Information Technology, Annamalai University, Annamalai Nagar, Tamil Nadu, India
E-Mail: alapatimail@gmail.com, rsuban82@gmail.com

(Received 12 September 2018; Revised 22 September 2018; Accepted 10 October 2018; Available online 17 October 2018)

***Abstract* - MANET routing is complex task and selecting secured route ought to be made sooner before the node leaves the network. Quick choices dependably redress network execution. Most MANET routing conventions are intended to work in a cordial and agreeable condition which makes them powerless against different assaults. Further, nodes need to forward data packets to different nodes to empower information correspondence between the nodes that are not in the radio scope of each other. Be that as it may, a node may decline to forward data packets or halfway do the sending or even endeavor to intrude on the system tasks. This is for the most part thought to be a sort of bad conduct which demonstrates the presence of maliciousnode in a system. Trust and Reputation would fill in as a noteworthy answer for these issues. Secured data transmission is a complex task in MANET as there is a maximum chance for attackers to crash the network. Taking in the system qualities and picking right routing choices at right occasions would be a noteworthy arrangement. In this work, we have completed a broad overview of fault tolerant methods connected to routing in MANETs. Because of the proximity of attackernodes, the procedure of administration disclosure is extraordinarily influenced, which may prompt poorer execution of the network. This may prompt less packet delivery proportion, throughput, expanded control overhead;add up to overhead and packet drops. Further, anchoring administration revelation task is exceptionally troublesome since, it includesthe notoriety of the extensive number of middle of the road nodes present in the system[3]. This paper presents a survey on different techniques for routing,key management and reductions method on packer droppings.**

Keywords: **MANETS, Routing, Key Management, Key Distribution, Routing Techniques, Packet Drops**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are exceptionally versatile nodes that speak with one another without depending on a prior network foundation[1]. With enormous system adaptability and node versatility, MANET routing presents another arrangement of nontrivial difficulties, for example, communication overhead, dynamic topology changes, and moderate network formation[2]. Since MANET accepts a convivial situation, it is powerless against assaults and maliciousnodes. MANET has transfer speed requirements yet it permits self-sufficient correspondence of versatile clients over it. Because of regular node development, and along change in system topology, the execution of the system goes unpredicted after some time[5]. In such a decentralized domain, routing and data transfer is relatively challenging issue[19]. The below fig.1 illustrates different routing methods.

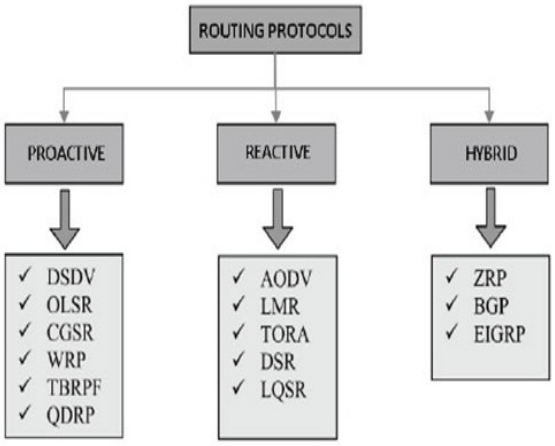

Fig. 1 Different Routing Methods

A MANET, because of its remarkable framework less trademark contrasted with different sorts of remote systems, can be exceptionally valuable for some applications in which no framework exists[21]. Thus, secure routing methods are required to give secure correspondence strength for multicast routing[6].

Dynamic and isolatedrisks accomplish more harm to specially appointed systems as contrast with wired systems. Dynamic assaults like unauthorized access, malicious node entry, man in the middle assault, packet drops. The key parts of system security are secrecy, verification, integrity, accessibility, non-disavowal,authorization,high quality[7].

The classification, validation, trustworthiness, accessibility and non-disavowal can be guarantee through cryptographic key administration known as hard security and access control, dependability and nature of data can be guarantee through trust administration known as delicate security[20]. The fig.2 illustrates different key management methods.

With the end goal to ensure specially appointed systems against narrow minded what's more, malicious conduct, and various secure conventions have been created[22]. These conventions utilize an assortment of cryptographic methods

to ensure the routing methods, which thusly secures the route, in this manner ensuring the information that streams over them. Packet dropping is a critical issue in MANET because of malicious nodes. Several methods are introduced for reducing packet droppings to increase system performance[24].

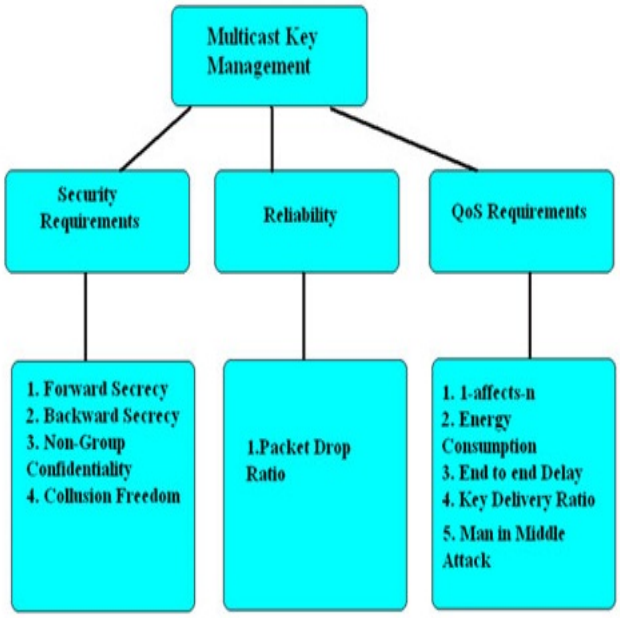

Fig. 2 Key Management methods

II. LITERATURE SURVEY

DSDV calculation establishesloop free route. Be that as it may, since relatively every node needs to include in route request and route reply methods, considering each node as a specific versatile node [8]. The main change in DSDV is the decrease in route updates because of the treatment of 'incremental refresh' packets which are similarly lesser in size [12]. The DSDV method likewise ensures loop free route yet it requests the keeping up of route tables in the individual versatile nodes [23]. Consequently, occasional and appropriate refreshing of routing tables upholds a more prominent overhead on the execution of a versatile node. The Authenticated Routing for Ad-hoc Networks (ARAN) proposed secure routing convention is an on-request routing convention that distinguishes and shields against noxious activities by maliciousnodes in the specially appointed system [11]. ARAN depends on the utilization of computerized endorsements where no system framework is present, however a earlier security coordination is normal [4]. ARAN gives verification, message trust and non- denial in specially appointed systems by utilizing a preliminary confirmation process that is trailed by a route instantiation process that ensures end-to-end intellect visioning of security administrations[12].

Khalili *et al.,* [1] proposed an ID based PKI with limited cryptography. Amid the system development, t nodes get the offer of top quality private key over the aggregate n nodes utilizing t-over-n plot. The nodes acquire their private key by consolidating the node ID with the t incomplete top quality private keys.

AnilKapil *et al.,* [2] proposed another area based pioneering routing convention named as Opportunistic and Area based Forwarding convention for Service arrangement (OLFServ). Their OLFServ convention fortifies both the disclosure and the summon of area attentive administrations in devious systems. Further, their convention actualizes self-pruning heuristics, which enables cell phones to choose regardless of whether they productively contribute in the conveyance of the messages they get from their neighbors[19].

Wan AnXoing *et al.,*[3] proposed another methodology for multi-way routing in versatile specially appointed systems. The route upkeep procedure of their convention gives data on the quality, toughness and strength of the ways.

Bing Wu *et al.,*[4] have built up a fault tolerant administration revelation convention for MANET utilizing majority of indexes. Registry nodes are chosen considering their weight esteems. The three layer model in this method comprises of routing, majority and administration layers from base to top. Their proposed convention includes two sections - choosing catalog nodes for building majorities, furthermore, benefit enrollment and queries utilizing the majorities.

D. Boneh *et al.,* [5] proposed a method that gives Certification Authority (CA) to share a secret key. It moreover provides end-to-end validation and authorize versatile user to assure the realness of client of the associate node. The critical preferred stand point of arrangement is to stay away from clients to create their own public keys and distribute these keys all through the system [14]. This method provides security method byselected organizations and is additionally reasonable different wireless networks.

Boukerche *et al.,* [6] improved a group based QoSrouting calculation for portable impromptu systems with a target of giving adaptation to non-critical failure, or, in other words include in giving QoS in the connection failureprone condition of versatile systems. Execution of this new fault tolerant group based QoS remote calculation is assessed by disappointment recovery time, dropped packets, throughput, and maintained stream data transfer capacity.

Pankaj Rohal *et al.,* [8] proposed a method to keep the flooding assault known as the neighbor suppression. In this each node screens and figures the rate of its neighbors' RREQ. In the event that this rate surpasses the predefined limit, the ID of this neighbor is recorded in the hub's memory[13]. Therefore every one of the solicitations originating from the hubs recorded in the rejection table is dropped. In any case, this technique comes up short against flooding assault in which the flooding rate is beneath the edge[16]. Subsequently to conquer this restriction, another methodology is utilized, in which factual examination is utilized to recognize vindictive RREQ messages.

Xin Ming Zhang *et al.*,[9] proposed an attack called blackhole assault. In a blackhole assault, in the wake of hearing the route request for packet in the system the assailant node professes to have a great degree short route to the goal. The aggressor does as such by sending a created RREP to the source node. In this RREP, the goal grouping number is set to be equivalent to or then again more noteworthy than the one contained in RREQ. This gives the source node the false impression that the vindictive node has the route to the goal. Subsequently the source node picks the course going through the assailant to send the information parcels. Presently since a large portion of the system activity goes through the malignant node, it can either drop the packets or control the activity in any capacity it needs. This assault is otherwise called the blackhole assault proposed by J. Newsome [10]. This assault is a refined variant of grey hole assault. Not at all like blackhole assault, here has the malicious node dropped just chosen packets and advances different packets, henceforth making the recognition of malicious node troublesome. This assault can be directed in different ways.

III. PROPOSED METHOD

Based on the survey done on routing mechanisms and key management techniques and packet drop reduction methods, novel methods need to be proposed for overcoming such issues.A novel technique need to be introduced for performing effective route establishment in which data can be securely transferred.

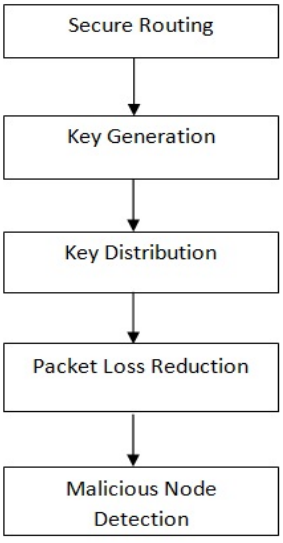

Fig. 3 Proposed Work Framework

For data transmission cryptographic methods are used for encrypting/decrypting the data so that unauthorized users cannot handle the data which results in increasing security levels.A novel method is to be proposed for detection of malicious nodes in the network to avoid data loss.The framework of the proposed work is illustrated in fig. 3.

IV. CONCLUSION

With the end goal to keep up the alternative idea of maintaining adhoc systems, in this paper we have utilized an irregular methodology of authorizing trust in the system. We have moved from the regular mechanism of accomplishing trust in the system by means of security to authorizing dependent capacity through joint effort. Every node in the network screens its encompassing neighbors and checks trust on them. These qualities are proliferated through the system alongside the information activity. These trust esteems are then associated with the nodes present in the MANET. This allows nodes to recover trustworthy routes from the available routes rather than standard most limited ways. In this paper, severalroutingconventions based on key plans are observed. Symmetric key plans indicate least computational quality as contrast with deviated and half and half key plans. Specially appointed systems are as often as possible focused by participating maliciousnodes to attack the system. A typical component to ensure these systems is using encryption and hashing mechanisms. In any case, the usage of these mechanisms by and large forces certain unessential requirements, which are considered as prohibitive for unarranged situations. Packet drop reduction methods are analyzed and need to be improved for increasing system performance.

REFERENCES

[1] Khalili, Katz, Jonathan and Arbaugh, A. William, “Towards secure key distribution in truly ad hoc networks”, *IEEE Workshop on Security and Assurance in ad hoc Networks* –2003.

[2] AnilKapil and SanjeevRana, “Identity-Based Key Management in MANETs using Public Key Cryptography”, *International Journal of Security*, Vol. 3, No.1. 2009.

[3] Wan AnXoing and Yao Huan Gong, “Secure and Highly Efficient Three Level Key Management Scheme for Manet”, *Wseas Transactions on Computers*, Vol. 10, No. 10, 2011.

[4] Bing, Jie Wu and Yuhong Dong, “An efficient group key management scheme for mobile ad hoc network”, *International Journal and Networks*, Vol. 2, No.3, 2008.

[5] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures, Advances in Cryptology–Crypto’04”, *Lecture Notes in Computer Science*, Vol. 3152, pp. 41–55, 2004,

[6] B.Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D.Turgut, “Routing protocols in ad hoc networks: A survey,” “*Elsevier Computer Networks*”, pp. 3032–3080, 2011.

[7] VeenaAnand and Suresh Chandra Gupta, “Performance of AODV, DSR and DSDV Protocols under varying node movement”, 2012.

[8] PankajRohal, RuchikaDahiya and PrashantDahiya, “Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV)”, *International Journal for Advance Research in Engineering and Technology*, Vol. 1, No.2, 2013.

[9] Xin Ming Zhang, En Bo Wang, Jing Xia, and Dan Keun Sung. “A Neighbor Coverage based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad hoc Networks” *International Journal of Engineering and Technology*, Vol.4, No. 5, 2012.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses”, *Proceeding of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259-268, 2004.

[11] K.Sanzgir, and B.Dahill, “A secure routing protocol for ad hoc networks”, *Proceeding of the 10th IEEE International Conference on Network Protocols*, pp.1-10, 2000.

[12] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure routing protocol Resilient to Byzantine failures", *Proceedings of ACM workshop on Wireless Security*, pp. 21-30, 2003.

[13] ImrichChlamtac, Marco Conti and Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges", *Elsevier Network Magazine*, Vol. 13, pp. 13-64, 2003.

[14] Y. Hu, A. Perrig and D. B Johnson, "Rushing attacks and defense in Wireless Ad Hoc Network Routing Protocol", *Proceedings of ACM workshop on wireless security*, pp. 30-40, 2003.

[15] JaydipSen, M. Girish Chandra, S.G Harihara, Harish Reddy and P. BalaMuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", *Proceedings of 6th International Conference on Information, Communications and Signal Processing*, 2007.

[16] Kummakasikit, M. Thipchaksurat, S. Varakulsiripunth, "Performance Improvement of Associativity-Based Routing Protocol for Mobile Ad Hoc Networks", *Fifth International Conference on Information, Communications and Signal Processing*, pp. 16 – 20, 2005.

[17] Detti, Blefari-Melazzi, N. Loreti, "Overlay, BoruvkaBased, "Ad-Hoc Multicast Protocol: Description and Performance Analysis", *International Conference on Communications*, pp. 5545 – 5552, 2007.

[18] SreeRangaRaju, Mankanala, Mungara, Jitendranath, "ZRP versus DSR and TORA: a comprehensive survey on ZRP performance", *10th IEEE Conference on Emerging Technologies and Factory Automation*,pp. 1024, 2005.

[19] Latiff, L.A. Ali, A. Ooi Chia-Ching and Fisal, "Development of an indoor GPS-free self-positioning system for mobile ad hoc network (MANET)", *13th IEEE International Conference on Networks*,2005.

[20] K.G.S. Venkatesan, R. Resmi, and R.Remya, "Anonymizing Geographic Routing for Preserving Location Privacy Using Unlink ability and Unobservability" in *IJACSSE*, Vol. 4, No.3, 2014.

[21] Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", *Sensors and Networks*, 5022-5039, 2009.

[22] Salmin Sultana, Gabriel Ghinita, ElisaBertino, and Mohamed Shehab, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks" *Journal Of Latex Class Files*, Vol. 6, No. 1, 2015.

[23] PushpendraNiranjan, rashantSrivastava, Raj kumarSoni, and Ram Pratap, "Detection of Wormhole Attack using Hopcount and Time delay Analysis" *International Journal of Scientific and Research Publications*, Vol. 2, No. 4, 2012.

[24] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure Network Provenance," *Proc. ACMSOSP*, pp. 295-310, 2011.