IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

A Study on Multipath Routing Security Protocols for Mobile Ad Hoc Networks

Y. Vasudeva Reddy[1*] and M. Nagendra[2]

[1*]Computer Science, Rayalaseema University, Kurnool, India
[2] Computer Science and Technology, Sri Krishnadevaraya University, Ananthapuramu, India

[*]*Corresponding Author: yvr.gpr@gmail.com, Tel.: +91-9989778399*

Available online at: www.ijcseonline.org

Received: 30/Nov/2017, Revised: 12/Dec/2017, Accepted: 24/Dec/2017, Published: 31/Dec/2017

***Abstract*—** Mobile ad hoc network (MANET) is a multi-hop wireless network that requires no infrastructure. The major issue in developing the routing protocols for the MANETs is their dynamic topology. The traditional single path routing protocols are not efficient for secure communication. Multipath routing protocols provide higher throughput and security than uni-path routing protocols in MANETs. The objective of the paper is to study various security attacks relevant to multipath routing in MANET which helps in developing a reliable, secure multipath routing protocol with significant performance in MANETs.

***Keywords* —** MANET, multipath routing, security, performance.

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) [1-5] is an instant wireless network requiring no infrastructure as shown in Figure 1. An important property of MANET is its dynamic topology. Also, due to the absence of fixed centralized administrative node, the networking functions like routing, security, etc. are handled by the nodes themselves. Each node in the MANET plays a dual role as a router and a host. The node becomes the host when it is the end node of communication, i.e., a source or a destination. The node acts as a router when it is the intermediate node of communication. As the MANETs can be setup easily and rapidly whenever the need arises, they find numerous applications like military communications, emergency and rescue operations, commercial applications and civilian applications [6].

Routing is an important networking functionality in MANETs. Almost all the routing protocols of MANETs are designed with the assumption that there are no malicious nodes in the network and all the nodes cooperate in forwarding the packets. But in practice, this assumption does not hold always. In presence of malicious nodes, the secure communication is not possible and the network performance degrades. It is very important to develop a secure routing protocol with the significant performance.

The traditional routing protocols used in MANET establish only one routing path between source and destination nodes and the path can be setup in three different ways: proactive, reactive and hybrid routing schemes.

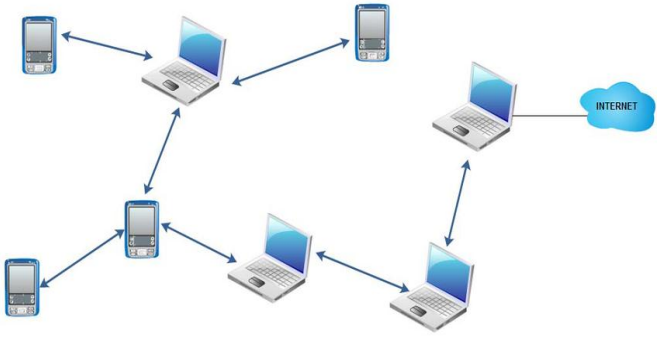

Figure 1. Mobile ad hoc network

In proactive routing, the paths are established during the network initial setup phase and are maintained till the network goes down. Under the maintenance of routing paths, each node exchanges topology information with other nodes. The benefit of proactive routing scheme is that the routes are available always between any pair of nodes which eliminates the delay of route discovery. But the problem with the proactive routing scheme is the routing overhead involved in route maintenance. On the other hand, reactive routing scheme discovers the route only when it is required and maintained as long as the data is transferring between source and destination. Reactive routing scheme adds route discovery delay but reduces the routing overhead involved in route maintenance. Finally, the hybrid routing scheme combines the best features of both proactive and reactive routing schemes to achieve the best performance. Some of the proactive routing protocols are Dynamic DSDV [7],

WRP [8], CGSR [9], GSR [10], FSR [11], HSR [12], LANMAR [13] and OLSR [14]. Reactive routing protocols are ABR [15], SSA [16], TORA [17], CBRP [18], DSR [19] and AODV [20]. The hybrid protocols are (DHAR) [21], ADV [22], ZRP [23], SHARP [24] and NAMP [25]. All these protocols discover multiple paths between source and destination but select only one best path based on certain criteria such as hop count, link quality, etc. When the path fails during data transmission due to node failure or link failure, the routing protocol either repairs the path or discovers another path between source and destination nodes. It results in delay which is not tolerable by delay-sensitive applications like voice over IP, video transmission etc. In order to ensure the quality of service of the applications in the MANETs, several researchers are recommending the usage of multipath routing protocols instead of traditional unipath routing protocols [1–4].

In multipath routing, at least two paths are established between source and destination and all the paths are used simultaneously to transmit the data between the nodes. Reliable transmission is possible with multipath routing scheme because when a path fails, data transmission can still happen through another path. Network throughput is increased with multipath routing as the data is transmitted through multiple different paths between source and destination. Multipath routing is best suitable for delay-sensitive applications in MANETs. Also, multipath routing scheme can provide security in a better way as a node in one path is malfunctioned or attacked, data can be transmitted securely through other safety paths. Compared to unipath routing scheme, it is difficult to attack the network using multipath routing approach.

There is a trade-off between security and performance of the network. If most secure communication is required, then performance of the network degrades because of processing delay and overhead involved in implementing the security scheme. To improve the performance of the network, security system can be compromised but it is dangerous for users as more security threats are possible. It is a challenging task for the researchers to develop a protocol which compromises between security and performance of the network. Multipath routing scheme is the best method to achieve the goal of secured communication with acceptable delay in MANETs.

The focus of the paper is to discuss various security threats and the possible solutions using multipath routing scheme in MANETs. Several researchers proposed various solutions for the security problems in multipath routing schemes. Organizational study of the multipath routing security problems and corresponding solutions is important for a researcher in this area. The paper discusses about various classifications of security attacks in multipath routing scheme. Also, the paper introduces taxonomy of all the attacks and solutions proposed so far in the literature. Finally, the paper provides the guidelines for developing solutions of multipath routing security problems in MANETs.

The remainder of the paper is organized as follows: section II presents fundamentals of multipath routing in the MANETs. The challenges of secure multipath routing protocols in MANETs are discussed in section III. The security problems in MANETs are given in section IV. Security problems relevant to routing in MANETs are presented in section V. The issues and solutions relevant to multipath routing in MANETs are given in section VI. The paper concludes with the section VII.

II. BACKGROUND KNOWLEDGE OF MULTIPATH ROUTING IN MANETS

An important property of multipath routing protocols is to find multiple disjoint paths between sender and receiver. Two routing paths are called disjoint if they have no common node and/or link. In case of non-disjoint paths, the common nodes or links get congested and the network performance degrades. There are two types of disjoint paths: node-disjoint paths and link-disjoint paths. The node-disjoint paths between a pair of sender and receiver nodes have no common node except source and destination nodes. The node-disjoint paths must ensure that at least one path remains available in case of a node failure. The link-disjoint paths have no common link in multiple paths, but common nodes might present. The link-disjoint paths must ensure that at least one path remains available in case of a link failure. The figure 2 illustrates the disjoint paths in the MANETs. In Fig. 2 (a), two node-disjoint paths P_1(S, A_1, A_2,..., A_n, D) and P_2(S, B_1, B_2, …, B_m, D) are shown and it can be observed that there is no common node present in paths P_1 and P_2. Similarly, Fig. 2 (b) shows two link-disjoint paths P_3(S-C_1, C_1-C_2, C_2-C_3, ..., C_n-D) and P_4(S-E_1, E_1-E_2, E_2-E_3, ..., E_m-D) that have no common link but may have common node as C_2. Some of the node-disjoint multipath routing protocols proposed for the MANETs are [26 – 28] and the link-disjoint paths are [29-30].

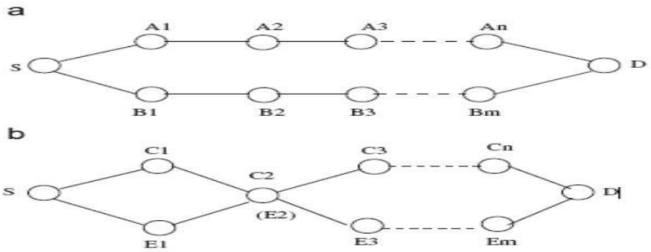

Figure 2. Illustration of disjoint paths: (a) node-disjoint paths (b) link-disjoint paths

The major benefits of multipath routing in MANETs are load-balancing, fault-tolerance and higher aggregate-bandwidth. Moreover, multipath routing protocols provide more security compared to unipath routing protocols in MANETs. Specifically, node-disjoint multiple paths are more secure than link-disjoint multiple paths between a single source and single destination node in MANET. Node-disjoint paths are also link-disjoint paths but not vice-versa because link-disjoint paths might contain a common node as shown in figure 2(b). If the common node is attacked then all the paths going through that node are affected.

III. MULTIPATH ROUTING SECURITY CHALLENGES IN MANETS

The unique characteristics of MANETs impose several security challenges. The researchers have to face the challenges to provide secure communication between any pair of nodes in the MANETs.

Absence of Infrastructure: As there is no fixed centralized wired infrastructure support in MANET, each node acts as a host and a router. When source and destination nodes are not directly reachable from each other, the intermediate nodes forward the packets between them. Source and destination nodes have to trust the intermediate nodes to transmit the data between them. An intruder can easily attack the intermediate nodes to steal the data of source and destination nodes. It is up to the sender and receiver nodes to take care of their secure communication as there is no centralized administration to save the data.

Multipath routing approach is better than unipath routing since the intruder must compromise at least 'n' nodes if there are 'n' node-disjoint paths between single sender-single receiver in the MANET. If one path is attacked, the data can be transmitted securely through the remaining paths from the sender to receiver since multiple paths are available in multipath routing scheme. Multipath routing security system fails only when all the paths are attacked by intruders. The researchers must design secured multipath routing protocols that can be operated completely in a decentralized administrative network.

Battery powered nodes: The nodes in the MANETs are battery powered. It is known fact that more battery power is consumed on networking functions than other functionalities like application running. Therefore, it might happen that some of the intermediate nodes do not forward the data packets between sender and receiver nodes to save their battery life. The selfish node attacks can cause the data loss. In multipath routing scheme, the selfish node attacks are possible only when every path includes at least one selfish node between sender and receiver nodes. The security protocol incurs additional processing overhead on the nodes which consumes the battery power. The researchers must consider the battery power of nodes as an important parameter while developing the secured multipath routing protocols for MANETs. Power conservative secured multipath routing protocols are attractive.

Node mobility: As the nodes are moving continuously from one location to other, the MANET topology changes dynamically. It allows any node to come in and go out of the network. More security attacks are possible in this kind of open environment of MANET. When a path fails due to a node displacement, the data transmission proceeds with other paths in multipath routing scheme in MANETs. The security solution must be adaptable to the dynamic topology environment of MANETs.

Wireless Link Quality: In MANETs, the wireless link has limited bandwidth and the link quality changes dynamically with noise, signal fading and interference. Most of the security attacks are based on link quality; particularly link-state routing protocols are more vulnerable. Security solutions must consider link quality as a parameter and the protocol providing both security and significant bandwidth of links is highly appreciable.

Multi-hop Communication: Each node in a MANET has a limited transmission range. When two nodes beyond the range of each other want to communicate, the intermediate nodes present between them must help in forwarding the packets. All the routing protocols designed so far in the literature assume that the nodes are honest and trust each other. In practice, this assumption does not hold. Trust based security attacks are most common in MANETs. The security solutions must consider node trust value as a parameter.

Network Freedom: Due to the lack of centralized administration, any node can join or leave the MANET. The freedom of network membership opens the doors for the attackers. The security solutions must define secure boundary of network.

IV. SECURITY PROBLEMS IN THE MANETS

There exist different types of security problems in the MANETs. Proper study of security attacks is needed for the researcher to develop the security solutions for the MANETs. This section presents various security problems relevant to multipath routing in MANETs.

A. Layer wise Security Attacks: As specified in [31], security attacks can be studied layer wise; physical layer attacks are eavesdropping, jamming, active interference; data link layer attacks occur due to selfish misbehavior of nodes and link traffic analysis; network layer attacks are wormhole, black hole, gray hole, Sybil, jellyfish, byzantine, link withholding, replay attacks, partitioning

attacks, location disclosure, link spoofing and rushing attacks; transport layer attacks include SYN flooding and session hijacking; application layer attacks include malicious code and repudiation. In addition, a few attacks such as denial of service and impersonation are considered as multilayer attacks. The focus of the paper is to study network layer attacks of multipath routing in MANETs.

B. Attacker based Security Problems: Based on the nature of attacker, another classification of security attacks is specified in [31] that includes two categories: passive attacks and active attacks. It is difficult to detect passive attacks because they do not change the data and do not interrupt the network operation. In contrast, active attacks modify the data and disturb the network operation. Passive attacks include eavesdropping and traffic analysis and monitoring. Active attacks include modifying the routing packets with false information, dropping the packets, etc. This paper discusses about active and passive attacks of multipath routing in MANETs.

C. Location based Security Attacks: The survey work [31] also specifies another classification of security attacks based on the location of attacker in the MANETs: internal and external attacks. The nodes present inside the MANET cause internal attacks. The nodes outside the MANET are the sources of external attacks. It is difficult to detect internal attacks compared to external attacks. The multipath routing security schemes must be able to handle both internal and external attacks.

V. ROUTING SECURITY PROBLEMS IN THE MANETS:

Routing attacks happen by violating the procedure of routing protocol. Based on the routing protocol being used in MANET, there exist different types of routing attacks. As specified in [32], a few common attacks of routing protocols include:

A. Routing Table Overflow Attacks: Each node in MANET acts as a router and a host. As per the routing protocol (proactive or reactive), each node maintains a routing table to discover and maintain the paths between a pair of nodes. As the routing table has fixed and limited size, the attacker node causes routing table overflow attacks by sending excessive route advertisement packets. As a result, new routes cannot be discovered.

B. Routing Table Poisoning: As the MANET has dynamic topology, the routing protocol must update the path as the topology changes. The routing protocol uses small control packets to update the paths as per the topology changes. The attacker modifies control packets so that nodes choose suboptimal routes or even network partition can happen.

C. Packet Replication: The routing paths are updated dynamically as the topology changes by exchanging small control packets. The attacker nodes replicate the expired packets so that the resources of network like bandwidth and node's battery power is unnecessarily wasted on processing these expired packets. Moreover, these replay attacks cause confusion in the routing process.

D. Rushing Attacks: On-demand routing protocols which discard the duplicate routing packets during the routing process are vulnerable to these attacks. Attacker node receives the route request packet from the source node and floods the packet quickly throughout the network than other nodes. As a result, the source node discovers the path that includes the attacker node. It is very difficult to detect and resolve this kind of attacks in MANETs.

E. Routing Cache Poisoning Attacks: The router nodes store routing table entries in router cache memory for quick processing of routing decisions. An attacker node may feed false information about routing paths or even delete or modify the entries in router cache memories. These attacks cause unnecessary bandwidth consumption, routing loops and other problems in the network. The on-demand routing protocols using promiscuous mode routing updates are more vulnerable to these attacks.

F. Packet Forwarding Attacks: These attacks are very difficult to detect and correct. Attacker node participates in the routing process and involves in the routing path from source to destination. When the attacker node receives a data packet to forward, simply the packet is dropped by the attacker. In case if the transmission is unreliable, then the source of data packet is unable to detect the packet loss.

G. Routing Protocol Specific Attacks: In MANETs, most of the routing attacks target a specific routing protocol like AODV, DSR, ARAN, ARIADNE, SEAD, OLSR, etc., because the routing protocols are developed to provide routing services without considering the security services. Routing protocol specific attacks are explained in detail in [32].

VI. SECURE MULTIPATH ROUTING PROTOCOLS:

Multipath routing protocols provide higher throughput, more reliable and secure transmissions over unipath routing

protocols in MANETs. It is not easy for the attacker to attack the network using multipath routing because the attacker has to compromise at least one node in 'n' different multiple paths from the source to destination. Even when a node is attacked in a path, it doesn't affect much the network performance because still n-1 paths are working well in multipath routing. A few security attacks like false routing information propagation, data packet drop, etc. can affect the performance of multipath routing in MANETs. The security attacks on multipath routing in MANETs can be studied in a systematic way by following the classification. As multipath routing protocols of MANETs are broadly categorized into two types: node-disjoint and link-disjoint paths, the security attacks can be studied exclusively for each type. Node-disjoint multipath routing security attacks and link-disjoint multipath routing security attacks form two major categories of security attacks on multipath routing in MANETs. As node-disjoint multipath routing scheme provides more security than link-disjoint routing schemes, researchers recommend to use node-disjoint multipath routing security solutions for the MANETs. Further, classification is based on type of routing scheme: proactive, reactive and hybrid schemes. In fact, multipath routing security problem is solved as single path security problem. In [33], an analysis of three secured multipath routing protocols, Secure Routing Protocol (SRP) [34], the multipath routing protocol of [35] and the secure multipath routing protocol (SecMR) [36], for defending DoS attacks is presented. In [37], a solution for the attacks of misbehaving nodes in multipath routing in MANETs is presented. The solution for the problem of using maximum number of secure multiple paths in MANETs is proposed in [38]. End-to-end feedback based security solution for reliable multipath routing in MANETs is proposed in [39].

A security solution for multipath routing in MANETs can be developed during route discovery and/or route maintenance phases. As security and performance are contradictory metrics to each other, it is a very challenging task for the researchers to develop a security solution with significant performance in MANETs. Moreover, the nodes in MANETs have limited resources of processing power, memory, battery power, etc. The security solution must impose overhead as low as possible and conserve the resources as much as possible. Detecting malicious nodes dropping data packets is a challenging task. Multipath routing security solutions must address the problems with misbehaving nodes present in the path from source to destination. The security solutions [33-39] proposed so far are focused on a specific routing attack. It is desirable to have a single solution to address maximum number of security problems of multipath routing in MANETs.

VII. CONCLUSIONS

Multipath routing approach provides higher throughput and security compared to traditional unipath routing approach used in MANETs. Since multiple paths are used simultaneously for data transmission between a source and destination, multipath routing provides better performance in MANETs. Security attacks relevant to multipath routing can degrade the performance of network. For reliable and secure communication with significant performance, security solutions are needed to assist the multipath routing from source to destination. This paper presents various attacks and a few solutions proposed in literature for multipath routing security in MANETs. It is observed that since data is transmitted through multiple paths simultaneously, it is very important to monitor the communication through each path and provide security to data. As multiple paths are discovered and maintained for data transmission between a pair of communicating nodes, security solutions must consider all relevant parameters like security, performance, QoS, etc for the optimal performance of network.

REFERENCES

[1] S. Sarkar and R. Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks," Ad Hoc Networks, vol. 37, pp. 209–227, Feb. 2016.

[2] P. K. Manohari and N. Ray, "Multipath routing protocols in MANETs: A study," in 2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016, 2016, pp. 91–96.

[3] P. K. Manohari and N. K. Ray, "EAOMDV: An energy efficient multipath routing protocol for MANET," in 2015 IEEE Power, Communication and Information Technology Conference, PCITC 2015 - Proceedings, 2016, pp. 710–715.

[4] B. Rajkumar and G. Narsimha, "Secure Multipath Routing and Data Transmission in MANET," Int. J. Netw. Virtual Organ., vol. 16, no. 3, pp. 236–252, 2016.

[5] P. R. and R. N., "An improved multipath MANET routing using link estimation and swarm intelligence," EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, p. 173, Dec. 2015.

[6] Y. V. R. and M. N. G Vijaya Kumar, "Current Research Work on Routing Protocols for MANET : A Literature Survey," International Journal on Computer Science and Engineering (IJCSE), vol. 2, no. 3, pp. 706–713, 2010.

[7] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," ACM SIGCOMM Computer Communication Review, vol. 24, no. 4, pp. 234–244, 1994.

[8] S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," Mobile Networks and Applications, vol. 1, no. 2, pp. 183–197, 1996.

[9] W. Liu, C. Chiang, H. Wu, and C. Gerla, "Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel," in Proc. IEEE SICON'97, 1997, pp. 197–211.

[10] T. W. Chen and M. Gerla, "Global state routing: A new routing scheme for ad-hoc wireless networks," in International Conference on Communications - Proceedings, 1998, vol. 1, pp. 171–175.

[11] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable routing strategies for ad hoc wireless networks," IEEE

Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1369–1379, 1999.

[12] M. Joa-Ng and I. T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1415–1425, 1999.

[13] G. Pei, M. Gerla, and X. Hong, "LANMAR: Landmark routing for large scale wireless Ad Hoc Networks with group mobility," in 2000 1st Annual Workshop on Mobile and Ad Hoc Networking and Computing, MobiHOC 2000, 2000, pp. 11–18.

[14] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," 5th IEEE Multi Topic Conference (INMIC 2001), p. 62, 2001.

[15] C.-K. Toh, "A Novel Distributed Routing Protocol To Support Ad-Hoc Mobile Computing," in Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications, 1996, pp. 480–486.

[16] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, "Signal stability-based adaptive routing (SSA) for ad hoc mobile networks," IEEE Personal Communications, vol. 4, no. 1, pp. 36–45, 1997.

[17] V. Park and M. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," … Annual Joint Conference of the IEEE …, pp. 1405–1413, 1997.

[18] T. Y. Jiang M, Li J, "Cluster Based Routing Protocol (CBRP)," IETF Draft, 1999. [Online]. Available: https://tools.ietf.org/wg/manet/draft-ietf-manet-cbrp-spec/. [Accessed: 25-Aug-2017].

[19] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, vol. 353, pp. 153–181, 1996.

[20] C. Perkings, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," Ietf Rfc 3561, pp. 1–37, 2003.

[21] A. B. McDonald and T. Znati, "A dual-hybrid adaptive routing strategy for wireless ad hoc networks," in 2000 IEEE Wireless Communications and Networking Conference, 2000, vol. 3, pp. 1125–1130.

[22] R. V. Boppana and S. P. Konduru, "An adaptive distance vector routing algorithm for mobile, ad hoc networks," in Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No.01CH37213), 2001, vol. 3, pp. 1753–1762.

[23] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," draftietfmanetzonezrp02 txt. p. 11, 2002.

[24] V. Ramasubramanian, Z. J. Haas, and E. G. Sirer, "SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks," in Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, 2003, pp. 303–314.

[25] A.-S. K. Pathan, M. M. Alam, M. M. Monowar, and M. F. Rabbi, "An efficient routing protocol for mobile ad hoc networks with neighbor awareness and multicasting," E-Tech 2004: An International Multi-Topic Conference, pp. 97–100, 2004.

[26] L. X. and L. Cuthbert, "On- demand node-disjoint multipath routing in wireless ad hoc networks," in In 29th Annual IEEE International Conference on Local Computer Networks, 2004, pp. 419–420.

[27] L. X. and L. Cuthbert, "Stable node-disjoint multipath routing with low overhead in mobile ad hoc networks," in Proceedings of the IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004, pp. 184–191.

[28] S. Lal, Chhagan, Vijay Laxmi, Manoj Gaur, "A node-disjoint multipath routing method based on AODV protocol for MANETs," in IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), 2012, pp. 399–405.

[29] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in Proceedings of the IEEE ICC, 2001, pp. 3201–3205.

[30] A. Nasipuri and S.R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks," in Proceedings of IEEE ICCCN'99, 1999, pp. 64–70.

[31] R. B. I. Saritha Reddy Venna, "A survey on security in mobile ad hoc networks," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 7, no. 1, pp. 135–140, 2016.

[32] K. P. Manikandan, R. Satyaprasad, and K. Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks," International Journal of Advanced Computer Science and Applications, vol. 2, no. 3, pp. 7–12, 2011.

[33] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Performance Analysis of Secure Multipath Routing Protocols for Mobile Ad Hoc Networks," Wired/ Wireless Internet Communications, Proceedings, vol. 3510, pp. 269–278, 2005.

[34] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris, "Secure Multipath Routing for Mobile Ad Hoc Networks," in Second Annual Conference on Wireless On-demand Network Systems and Services, 2005, pp. 89–96.

[35] M. Burmester and T. Van Les, "Secure Multipath Communication in Mobile Ad Hoc Networks," in Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 04), 2004, pp. 405–409.

[36] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR - a secure multipath routing protocol for ad hoc networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87–99, Jan. 2007.

[37] M. Kefayati, H. R. Rabiee, and A. Khonsari, "Misbehavior Resilient Multi-path Data Transmission in Mobile Ad-hoc Networks Categories and Subject Descriptors," Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, pp. 91–100, 2006.

[38] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks," in Proceedings - IEEE INFOCOM, 2004, vol. 4, pp. 2404–2413.

[39] L. Chen and J. Leneutre, "On Multipath Routing in Multihop Wireless Networks: Security, Performance, and Their Tradeoff," EURASIP Journal on Wireless Communications and Networking, vol. 2009, no. 6, pp. 1–13, 2009.

Authors Profile

Y. Vasudeva Reddy received MCA (Master of Computer Applications) and M.Phil (Computer Science) degree in 2005 and 2009, respectively. Presently pursuing Doctorate Degree (Ph.D) in Computer Science from Rayalaseema University, Kurnool. His research interest includes Wireless networks, Security, Routing Protocols.

Prof. M. Nagendra received Ph.D in Computer Science in 2008, M.Phil (Maths) and M.Sc (Maths) from S.K.University, Anantapur. He is working as Professor & HOD in the Department of Computer Sciece and Technology, S.K.University, Anantapur. His research interest includes computer networks and data mining. He is presently guiding 12 Ph.D scholars and 14 M.Phil scholars.

