International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 7, July - 2013

Study Of Vulnerabilities And Routing Issues In Mobile Adhoc Network

Najiya Sultana
Research Scholar,
Janardan Rai Nagar Rajasthan Vidyapeeth University
Udaipur, India

Prof. Shiv Singh Sarangdevot
Vice Chancellor
Janardan Rai Nagar Rajasthan Vidyapeeth University
Udaipur, India

***Abstract*— With the modernization of the wireless communication system, mobile adhoc network (MANET) has gain a pace in the area of communication system. Conceptualized with infrastructureless networking system, every mobile nodes in MANET participate in the process of network behave both as host as well as router and therefore, it is guided by the communication principles to forward the packet to other nodes and hence formulate networking phenomenon. The area of MANET has already found its scope in Military Battlefield, Sensor Networks, Commercial Sector, Medical Service, and Personal Area Network. Although, the research attempts in MANET is more than a decade old, but still commercialization of the technology are yet to be seen and therefore, due to novelty nature of the technology, MANET is also shrouded by various issues. Therefore, this paper discusses on the implicit understanding of literatures for maintaining security in routing protocols in MANET.**

Keywords-component: Routing, MANET, security

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is self-configuring infrastructureless network of mobile devices connected by wireless. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features [1] Unreliability of wireless links between nodes, constantly changing topology, and lack of incorporation of security features. According to security information with respect to MANET network are vulnerable compromises or physical capture, especially at the end of low-end devices due to weak protection. Intruders enter into the network and poses weakest link and incur a domino effect of security in the network. According to wireless channel is concerned bandwidth is one of constrained and use to share among multiple different network nodes. There is also one more restriction that is computation capability; like low-end devices for e.g. PDAs, can hardly perform low computation due to this way they usually use asymmetric cryptographic computation which is bit low complex, because mobile devices have very limited energy resources due to this way mostly mobile devices powered by batteries. The wireless medium as compared to wireline network node mobility more dynamics in mobile ah hoc networks. The network topology is highly dynamic due to free movement in the network like nodes can frequently join or leave, as well as in the network by their own will. There are also interferences in the wireless channel due to this way error, exhibiting volatile characteristics in terms of bandwidth and delay occurs. Due to such dynamic behaviors mobile users request for security services at any anytime or anywhere whenever they move from one place to another in the network.

Among all these security services, authentication is probably the most important and complex issue in MANETs because it is the bootstrap of the whole security system. Once authentication is achieved in MANET then confidentiality is just a matter of encrypting algorithm on the session by using keys. These security services can be provided singly or in combination, it only depends on our requirements. It is also true that security has long been an active research topic in wireline networks; but due to unique characteristics of MANET there are many challenges because of its self organizing behavior. These challenges are shared wireless medium, highly dynamic network topology, stringent resource constraints and open network architecture. It's true that existing security solutions for wired networks do not directly apply to the Mobile ad hoc networks domain.

II. SECURITY ON ROUTING

In an adhoc network, all the nodes may not be within the transmission range of each other; hence, nodes are often required to forward network traffic on behalf of other nodes. Consider for example the scenario in Fig 1, if node S sends data to node D, which is three hops away, the data traffic will get to its destination only of A and B forward it. The process of forwarding network traffic from source to destination is termed routing.

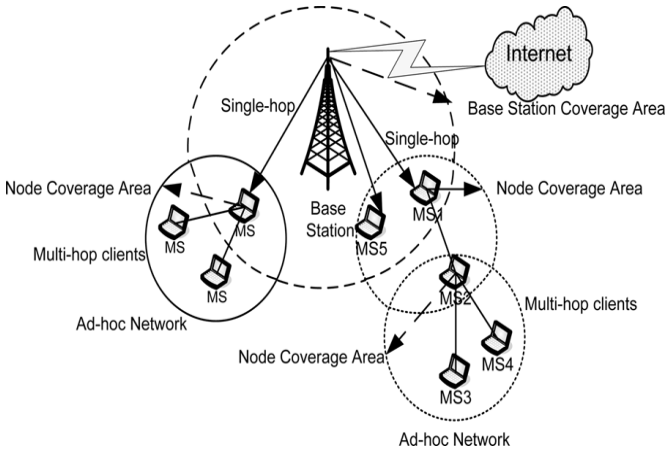

Figure 1 Multihop Scenario

There are two general categories of MANET routing protocols: topology-based and position-based routing protocols. We present a brief overview of each group below. Before proceeding, it is fitting to list some desirable qualitative properties of MANET routing protocols. This list is adopted from an Internet Engineering Task Force (IETF) MANET Working Group memo [2].

- *Demand-based operation*: In order to utilize network energy and bandwidth more efficiently, it is desirable that MANET routing algorithms adapt to the network traffic pattern on a demand or need basis rather than maintaining routing between all nodes at all time.
- *Loop-free*: It is desirable that routing protocols prevent packets from circling around in a network for arbitrary time periods.
- *"Sleep" period operation*: It may be necessary for reasons such as the need for energy conservation for nodes to stop transmitting or receiving signals for arbitrary time periods. Routing protocols should be able to accommodate sleep periods without adverse consequences.
- *Proactive operation*: This is the IP-side of demand-based operation. In cases where the additional latency, which demand-based operations incurred, may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations.
- *Security*: It is desirable that routing protocols provide security mechanisms to prohibit disruption or modification of the protocol operations.

In addition to the mentioned routing protocols for MANET, there are some other routing protocols that do not rely on any traditional routing mechanisms, instead rely on the location awareness of the participating nodes in the network. Generally, in traditional MANETs, the nodes are addressed only with their IP addresses. But, in case of location-aware routing mechanisms, the nodes are often aware of their exact physical locations in the three-dimensional world. This capability might be introduced in the nodes using Global Positioning System (GPS) or with any other geometric methods. Based on these concepts, several geo-cast and location-aware routing protocols have already been proposed. The major feature of these routing protocols is that, when a node knows about the location of a particular destination, it can direct the packets toward that particular direction from its current position, without using any route discovery mechanism. Recently, some of the researchers proposed some location-aware protocols that are based on these sorts of idea. Some of the examples of them are Geographic Distance Routing (GEDIR)[3], Location-Aided Routing (LAR)[4], Greedy Perimeter Stateless Routing (GPSR)[5], Geo-GRID[6], Geographical Routing Algorithm (GRA)[7], etc. Other than these, there are a number of multicast routing protocols for MANET. Some of the mentionable multicast routing protocols are: Location-Based Multicast Protocol (LBM)[8], Multicast Core Extraction Distributed Ad hoc Routing (MCEDAR)[9], Ad hoc Multicast Routing protocol utilizing Increasing id-numbers (AMRIS)[10], Associativity-Based Ad hoc Multicast (ABAM)[11], Multicast Ad hoc On-Demand Distance-Vector (MAODV) routing [12],Differential Destination Multicast (DDM)[13],On-Demand Multicast Routing Protocol (ODMRP)[14], Adaptive Demand-driven Multicast Routing (ADMR) protocol [15], Ad hoc Multicast Routing protocol (AMRoute)[16] Dynamic Core-based Multicast routing Protocol (DCMP)[17], Preferred Link-Based Multicast protocol (PLBM)[18] etc. Some of these multi cast protocols use location information and some are based on other routing protocols or developed just as the extension of another unicast routing protocol. For example, MAODV is the Multicast-supporting version of AODV

III. PRELIMINARY STUDY

In MANETs, some form of routing protocol is required in order to dynamically detect the multi-hop paths through which packets can be sent from one node to another. Active research work for MANETs is carrying on mainly in the fields of Medium Access Control (MAC), routing, resource management, power control, and security. Because of the importance of routing protocols in dynamic multi-hop networks, a lot of MANET routing protocols have been proposed in the last few years. Considering the special properties of MANET, when thinking about any routing protocol, generally the following properties are expected, though all of these might not be possible to incorporate in a single solution.

- A routing protocol for MANET should be distributed in manner in order to increase its reliability.
- A routing protocol must be designed considering unidirectional links because wireless medium may cause a wireless link to be opened in uni-direction only due to physical factors.
- The routing protocol should be power-efficient.
- The routing protocol should consider its security.
- A hybrid routing protocol should be much more reactive than proactive to avoid overhead.
- A routing protocol should be aware of Quality of Service (QoS).

There are basically two categories of routing protocols for MANETs:

1. Table Driven (Proactive): DSDV, GSR, WRP
2. Source Initiated On-Demand (Reactive): ABR, AODV, DSR, LAR

Based on the method of delivery of data packets from the source to destination, classification of MANET routing protocols could be done as follows:

- Unicast Routing Protocols: The routing protocols that consider sending information packets to a single destination from a single source.
- Multicast Routing Protocols: Multicast is the delivery of information to a group of destinations simultaneously, using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split. Multicast routing protocols for MANET use both multicast and unicast for data transmission.

Multicast routing protocols for MANET can be classified again into two categories: Tree-based multicast protocol and Mesh-based multicast protocol. Mesh-based routing protocols use several routes to reach a destination while the tree-based protocols maintain only one path. Much of the research has been done focusing on the efficiency of the MANETs. There are quite a number of routing protocols that are excellent in terms of efficiency. But the security requirements of these protocols changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To address these concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD), Ariadne, and Authenticated Routing for Ad hoc Networks (ARAN), Secure Ad hoc On-Demand Distance Vector Routing (SAODV), and Secure Routing Protocol (SRP). Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency are primary point of concern in implementing these protocols. Hence, there is a need for review. Mobile ad hoc network can be subject to many types of attacks. In Mobile ad hoc network, attacks can be classified into Passive Attacks and Active Attacks. Brief introduction of both attacks are as follow:

A. Passive Attacks

In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. The attacker only looks and watches the transmission and does not try to modify or change the data packets. Two types of passive attacks are:

- Traffic analysis: In this attack, attacker monitors packet transmission to infer important information such as a source, destination and source-destination pair.
- Eavesdropping: In Eavesdropping, attackers obtain some confidential information e.g. private key, public key, location or even password of the node that should be kept secret during transmission.

B. Security Services

Security services include the functionality required to provide a secure networking environment. The main security services can be summarized as follows:

- Authentication: This service verifies a user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each is the entity it claims to be. Secondly, it must assure that a third party does not interfere by impersonating one of the two legitimate parties for the purpose of authorized transmission and reception. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates. Details of the construction and operation of digital signatures can be found in RFC2560.
- Confidentiality: This service ensures that the data/information transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques such as only legitimate users can analyze and understand the transmission.
- Integrity: The function of integrity control is to assure that the data is received in verbatim as sent by authorized party. The data received contains no modification, insertion or deletion.
- Access Control: This service limits and controls the access of such a resource, which can be a host system or an application.
- Availability: This involves making the network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.

C. Active Attacks

In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks. Various types of active attacks are:

- Sinkhole Attack: A sinkhole node tries to attract the data toward itself from all neighboring nodes. In this attack, a malicious node generates fake routing information and show itself as legal nodes for the route. Sinkhole node attempts to draw all network traffic according to itself, modifies the data packets, decrease the network life time,

create complicated network and finally destroy the network.

- Flooding Attack: In this attack, a malicious node may also inject false packets to consume the available resources onto the network, so that valid user can not able to use the network resources for valid communication. The flooding attack is possible in all most all the on demand routing protocols such as SRP, SAODV, and ARAN etc.
- Replay Attack: This attack usually targets the freshness of routes. In this attack an attacker firstly record the message and then resend the old message to the other nodes to make update their routing table to stale routes.
- Rushing Attack In Rushing attack, attacker forward routing packets as quick as possible to gain access to multicast forwarding group before the legal node .By this way rushing attack can slow down the performance of network .The rushing attack can act as an effective DoS attack against all currently proposed on demand MANET routing protocol.

C. Common attacks in MANETs

- Denial-of-service with modified source route: In the denial-of-service, a malicious node in between can successfully send an erroneous route message to the source route to disrupt the service.
- Tunneling Attack: In tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes.
- Wormhole Attack: In Wormhole an attacker records packet at one location in the network, tunnels them to another location, and retransmits them back into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality
- Black hole Attack: In Black-hole attack a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept and in this way it can compromise the service.
- Spoofing Attack: In Spoofing a single malicious node in the ad hoc network can spoof the nodes identity in order to forward packets through it. Later the information can be used to create DoS attacks.

IV. Related Work

Panagiotis Papadimitratos e.t. al [19] has presented a route discovery protocol that is considered one of the standard work. John Marshall e.t. al [20] has proposed in this paper, the SRP algorithm for routing in ad hoc networks. Oscar F. Gonzalez e.t al [21] presented a mechanism that enables the detection of nodes that exhibit packet forwarding misbehavior. Stephan Eicher e.t. al [22] has introduced a novel secure routing protocol based on AODV for infrastructure-based MANETs is proposed. M. Rajesh Babu e.t. al [23] has proposed in this paper to develop an Energy Efficient Secure Authenticated Routing Protocol (EESARP). Steffen Reidt e.t.al [24] has introduced a trust metric in the cluster head selection process to securely determine constituting nodes in a distributed Trust Autho rity (TA) for MANETs. Muhammad Nawaz Khan e.t. al [25] has proposed distributed-ID, a smart agent in each mobile node analyzes the routing packets. Lu Jin e.t. al [26] they introduced on the securing the delivery of routing packets and the strategy of determine the most secure routes. Panagiotis Papadimitratos e.t. al [27] has propose the securing the delivery of routing packets and the strategy of determine the most secure routes. Shivasharanappa Allur e.t. al [28] has proposed a cross-layer design to achieve an unswerving data transmission in ADHOC networks. Venkat Balakrishnan e.t. al [29] they introduced Trust Enhanced security Architecture for MANET (TEAM), in which a trust model is overlaid on the following security models key management mechanism, secure routing protocol, and cooperation model. Kimaya Sanzgiri e.t. al [30] they are introduced solution to one, the managed-open scenario where no network infrastructure is pre-deployed, but a small amount of prior security coordination is expected. Poonam Yadav e.t. al[31] has introduced in this paper on demand routing protocols AODV, DSR and DYMO based on IEEE 802.11 are examined and characteristic summary of these routing protocols is presented. Parma Nand e.t. al [32] have introduced in this paper on demand routing protocols AODV, DSR and DYMO. David B. Johnson e.t. al [33] has presents a protocol for routing in ad hoc networks that uses dynamic source routing. Xiaodong Lin e.t. al [34] has present a novel anonymous secure routing protocol for mobile ad hoc networks (MANETs). Xu Su e.t .al [35] has proposed mechanisms to complement the existing secure routing protocols to resist the creation of in-band tunnels. Mohd Anuar Jaafar e.t.al [36] they introduced some evaluation and performance comparisons of AODV, SAODV and A-SAODV routing protocols in MANETs. Umang singh e.t.al [37] has introduced in this paper, various existing routing protocols were reviewed. Julien Francq e.t. al [38] has proposed countermeasure provides a high level of fault detection. Karim El Defrawy e.t. al [39] has presents the PRISM protocol which supports anonymous reactive routing in MANETs. Satoshi Kurosawa e.t. al [40] has proposed an anomaly detection scheme using dynamic training method. Amit N. Thakare e.t. al [41] has introduced in this paper, an attempt has been made to compare the performance of two prominent on demand reactive routing protocols for MANETs. Kimaya Sanzgiri e.t. al [42] has proposed propose a solution to one, the managed-open scenario where no network infrastructure is pre-deployed.

V. Conclusion

This paper presents a number of routing protocols for MANET, which are broadly categorized as proactive and reactive. Although, there was a massive research work in past that has also concentrated on addressing security issues in Mobile Adhoc Network, but majority of the prior studies are investigated to found various technical infeasibilities when it comes to computation, reliability, and much more sophisticated nature of study. Computation issues was found as majority of the prior study has deployed a strong usages of cryptography, while reliability issues was explored while

majority of the previous work has stressed on designing Intrusion Detection/prevention system that actually do not consider much critical parameters like selfish node, uncertain behaviour of mobile nodes, trivial identification of roles of selfish node, erroneous node, or malicious nodes. Therefore, the proposed work is done by considering all the above mentioned issues that has not been addressed much effectively in the prior studies.

REFERENCES

[1] Mishra,A., Nadkarni. K.M., "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
[2] Corson, S., Macker, J., "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations", Internet Request for Comments (RFC 2501), 1999.
[3] Lin, X., Stojmenovic, I., "GEDIR: Loop-Free Location Based Routing in Wireless Networks", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, pp.1025–1028, 1999
[4] Ko, Y-B., Vaidya, NH., "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks", Wireless Networks, Vol 6, pp. 307–321, 2000
[5] Karp, B., Kung, HT., "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks."ACM MOBICOM , pp.243–254, 2000
[6] Liao, W-H., Tseng, Y-C., Lo K-L., Sheu J-P., "GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks based on GRID", Journal of Internet Technology, Volume 1, Issue 2:23–32, 2000
[7] Jain, R., Puri, A,, Sengupta, R., "Geographical Routing Using Partial Information for Wireless Ad Hoc Networks", IEEE Personal Communications, Vol. 8, Issue 1, pp. 48–57, 2001
[8] Ko, Y-B., Vaidya, NH., "Location-based multicast in mobile ad hoc networks", Technical Report TR98-018, Texas A&M University, 1998
[50] Sinha, P., Sivakumar, R., Bharghavan, V., "MCEDAR: Multicast Core-Extraction Distributed Ad Hoc Routing", Proceedings of IEEE WCNC, Vol 3, pp. 1313–1317, 1999
[10] Wu, C.W., Tay TC., AMRIS: A Multicast Protocol for Ad Hoc Wireless Networks. IEEE MILCOM 1999, Volume 1, pp. 25–29, 1999
[11] Toh, C-K., Guichal, G., Bunchua, S., "ABAM: On-Demand Associativity-Based Multicast Routing for Ad Hoc Mobile Networks", Proceedings of IEEE VTS-Fall VTC, Vol. 3, pp. 987–993
[12] Royer, E.M., Perkins, C.E, "Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing", IETF Draft, draft-ietf-manet-maodv-00,availableat, 2012
[13] Ji, L., Corson, M.S., "Differential DestinationMulticast-A MANETMulticast Routing Protocol for Small Groups", Proceedings of IEEE INFOCOM, Vol 2, pp. 1192–1201, 2001
[14] Lee, S., Su, W., Gerla, M., "On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks", ACM/Kluwer Mobile Networks and Applications (MONET), Vol. 7, Issue 6, pp. 441–453, 2002
[15] Jetcheva, J.G., Johnson, D.B., "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks", Proceedings of ACM MobiHoc, pp.33–44, 2001
[16] Xie, J., Talpade, R.R., Mcauley, A,, Liu, M., "AMRoute: Ad Hoc Multicast Routing Protocol. Mobile Networks and Applications, Vol. 7, Issue 6, pp. 429–439, 2002
[17] Das, S.K., Manoj, B.S., Murthy, C.S.R., "A Dynamic Core Based Multicast Routing Protocol for Ad Hoc Wireless Networks. Proceedings of ACM MobiHoc, pp. 24–35, 2002
[18] Sisodia, R.S., Karthigeyan, I., Manoj, B.S., Murthy, C.S.R.,"A Preferred Link Based Multicast Protocol for Wireless Mobile Ad Hoc Networks", Proceedings of IEEE ICC 2003, Vol. l3, 2003
[19] Papadimitratos,P e.t.al. "Secure Routing for Mobile Ad hoc Networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 2002.
[20] Marshall, j e.t.al, "Identifying flaws in the secure routing protocol", Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International, 2003
[21] Oscar, F., Gonzalez., Howarth,M., Pavlou,G., "Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", Springer-Verlag Berlin Heidelberg, 2007
[22] Eichler, S. e.t. al., "Secure Routing in a Vehicular Ad Hoc Network". Vehicular Technology conference, 2004. VTC2004-Fall. 2004 IEEE 60th Date of Conference, 2004.
[23] Babu.M.R e.t. al., "An Energy Efficient Secure Authenticated Routing Protocol for Mobile Adhoc Networks", International Journal of Reviews in Computing 30th September 2011. Vol. 7, 2004
[24] Reidt.S e.t.al., "Efficient, Reliable and Secure Distributed Protocols for MANETs. Mobile Technology", Applications and Systems, 2005 2nd International Conference on Date of Conference, 2005.
[25] Khan.M.N e.t. al. "Intrusion Detection System for Ad hoc Mobile Networks. Information Technology: Research and Education, 2005. ITRE 2005. 3rd International Conference on Date of Conference, 2005.
[26] Jin,L e.t. al "Implementing and Evaluating An Adaptive Secure Routing Protocol for Mobile Ad Hoc Network", Wireless Telecommunications Symposium, 2006. WTS'06 Date of Conference, 2006.
[27] Papadimitratos.P., "How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET", 2009
[28] Allur.S e.t. al, "Efficient SNR/RP Attentive Routing Algorithm: Cross-Layer Design for Adhoc Networks," Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on Date of Conference, 2006.
[29] Balakrishnan,V., Varadharajan,V., Tupakula,U., Lucs,P "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks", IEEE, 2007
[30] Sanzgiri,K., Dahill,B., "A Secure Routing Protocol for Ad Hoc Networks", 2007

[31] Yadav,P., Gill,R,K., Kumar, N., "A Fuzzy Based Approach to Detect Black hole Attack", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol 2, Issue-3, 2012
[32] Nand,P et.al., "Performance study of Broadcast based Mobile Adhoc Routing Protocols AODV, DSR and DYMO", Wireless Pervasive Computing, 2007. ISWPC '07. 2nd International Symposium on Date of Conference: 5-7.2007.
[33] Johnson.D.B e.t.al, "Dynamic Source Routing in Ad Hoc Wireless Networks", Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on Date of Conference, 2007.
[34] Lin, X e.t .al, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks", Communications, 2007. ICC '07. IEEE International Conference on Date of Conference,2007
[35] Su,X e.t .al., "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks," Communications, 2007. ICC '07.IEEE International Conference on DateofConference, 2007.
[36] Jaafar,M.A e.t.al., "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", Communications Magazine, IEEE Date of Publication, 2008.
[37] Singh,U e.t.al, "secure routing protocols in mobile adhoc NETWORKS-A SURVEY AND TAXANOMY. Wireless Communications and Networking Conference, 2008. WCNC2008. IEEE Date of Conference, 2008.
[38] Francq,J e.t. al., "Error Detection for Borrow-Save Adders Dedicated to ECC Unit", Fault Diagnosis and Tolerance in Cryptography, 2008. FDTC '08. 5th Workshop on Date of Conference, 2008.
[39] Defrawy.K.E e.t. al, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", Risks and Security of Internet and Systems, 2008. CRiSIS '08. Third International Conference on Date of Conference, 2008.
[40] Kurosawa,S e.t. al., "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", Networks, 2008. ICON 2008. 16th IEEE International Conference on Date of Conference,. 2008.
[41] Thakare,A.N e.t. al., "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks", Advanced Information Networking and Applications Workshops, 2009.WAINA'09.International Conference on Date of Conference, 2009.
[42] Sanzgiri, K e.t. al, "A Secure Routing Protocol for Ad Hoc Networks", Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th International Conference on Date of Conference, 2009.

Najiya Sultana has 5 years teaching experience at degree level. She has completed MCA in 2005 and M. Phil. In 2010. She is pursuing Ph. D. from Rajasthan Vidyapeeth University, Udaipur. She has attended 5 international conferences and 2 national conferences. She is a member of CSI. Her research areas of interest are Ad Hoc networks, network security and security protocols.

Prof. Shiv Singh Sarangdevot is working as a Vice Chancellor of Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur. He has completed Doctor of Philosophy in Computer Science, Master of Computer Application, and Human Resource Management. He has 26 years of teaching experience. He has also 10 years of wide industrial experience with rich 21 years in research domain. His area of specialization includes Internet & E-Commerce, Software Engineering, ERP and SAP, Research Techniques, Artificial Intelligence, and Networking. He has also published 8 books and 78 research papers till date.