A Review of Routing Protocols for Mobile Ad Hoc Networks

ANUJ K. GUPTA HARSH SADAWARTI ANIL K. VERMA
RIMT-IET RIMT-IET Thapar University

Abstract: A number of routing protocols has been proposed in recent years for possible use of Mobile Ad Hoc Networks in various application areas such as military, govt. etc. In this paper we have presented a comprehensive review of these protocols with a particular focus on their security aspects. Further we have presented a comparison of some of the existing Routing Protocols of MANETs. The base criteria for comparison is routing methodologies and the information used to make routing decisions. All the protocols have to meet five security requirements: confidentiality, integrity, authentication, non-repudiation and availability, with respect to which the analyses of secure versions of proposed protocols are discussed.

Keywords: - Routing Protocols, Network attacks & Defense, AODV, DSDV, DSR, SRP, TORA, ZRP.

1 Introduction

A Mobile Ad Hoc Network (MANET) or spontaneous network is an infrastructure less, self-organized and multi-hop network with rapidly changing topology causing the wireless links to be broken and re-established on-the-fly. A key issue is the necessity that the Routing Protocol (RP) must be able to respond rapidly to the topological changes in the network. In these networks, each node must be capable of acting as a router. As a result of limited bandwidth of nodes, the source and destination may have to communicate via intermediate nodes [19]. Routing in MANETs has been an active area of research and in recent years numerous RPs have been introduced for addressing the problems of routing, reviewed in later sections. These protocols are divided into two broad classes – Reactive and Proactive [4].

In Reactive or on-demand RPs the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV). Wherein Proactive or Table-driven RPs the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and Destination Sequenced Distance Vector Protocol (DSDV). All these protocols are quite insecure because attackers can easily obtain information about the network topology [6]. In Section 2, first we focus on security aspects of MANET Routing Protocols and later in Section 3 we will present classification of the existing RPs, their types and review their characteristics. It also explores some of the proposed secure Routing Protocols, and Section 4 gives the qualitative comparison of their characteristics & categorizes them accordingly to their routing strategies & relationships [9]. Section 5 shows some assumptions in form of a chart based on the performance of Routing Protocols in terms of mobility and network size.

2 Network attacks & Defense

Several kinds of attacks compromise the safe exchange of information in MANETs, which can be categorized using different criteria. The attacks are generally classified into two types- Passive and Active. A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated [34]. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks. An Active Attack, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified [5]. To combat the vulnerabilities faced during these attacks, Routing Protocols have to meet the following security requirements:

- *Confidentiality*: Protection of any information from being exposed to unintended entities. In ad-hoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.
- *Integrity*: Message being transmitted is never altered.
- *Authentication*: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.
- *Non-repudiation:* Ensures that sending and receiving parties can never deny ever sending or receiving the message.
- *Availability:* Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack.

Table 1 outlines a brief overview of the more prominent attacks prevalent against ad-hoc networks, most of which are active [20].

Table 1: Ad Hoc Network Attacks

Black hole attack [21]	A malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker could cause the route to all nodes in an area of the network to point into that area when in fact the destination is outside the area.
Worm hole attack [6]	A pair of malicious nodes connected through a private network could record packets at one location in the network, forward them to another location through the private network and rebroadcasts them into the network
Routing table overflow [22]	The attacker attempts to create routes to fictitious nodes. The goal is to create enough routes to prevent new routes from being created.
Session hijacking [16]	The attacker appears to be an authentic node when the session starts and hijack the session.
Sleep deprivation [8]	An attacker can attempt to consume batteries by requesting routes, or by forwarding unnecessary packets to the node using, for example, a black hole attack
Location disclosure attack [23]	It can reveal something about the locations of nodes or the structure of the network. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node
Denial of Service (DoS) [24]	The malicious node prevents or prohibits the normal communication in a network. DoS attacks can be launched at any layer of an ad hoc network to exhaust node resources.
Jamming [18]	The attacker sends signals of similar frequency in which the sender and receiver communicate and causes a lot of errors in transmission.
Spoofing [18]	The attacker steals the identity of an authorized node to gain access to the network & disturbs the traffic.

These are the different digital attacks developed to undermine the security of mobile Ad hoc Networks. Table 2 summarizes the routing protocols in terms of proposed solutions to withstand different network attacks [4].

Table 2: Defense against network attacks

Attack	***Proposed Routing Protocol***
Black hole	CONFIDANT, OSRP
Worm hole	SEAD, Packet Leashes
Resource Consumption	SEAD [11]
Location Disclosure	SRP
Routing attacks	SEAD, ARAN, ARIADNE
Repudiation	ARAN
DoS	SEAD, ARIADNE, SRP
Impersonation	ARAN
Routing table poisoning	ARAN, SRP, ARIADNE, OSRP

Various routing protocols [10] have been proposed to achieve secure routing in an ad hoc network. These protocols are discussed in detail in nest section.

3 Routing Protocols for MANETs

This section will discuss the classification of existing Wireless Ad hoc RPs, their characteristic features & types. The Routing Protocols for ad hoc wireless networks can be divided into three categories based on the routing information update mechanism. They could be Reactive (On-demand), Proactive (Table-driven) or Hybrid.

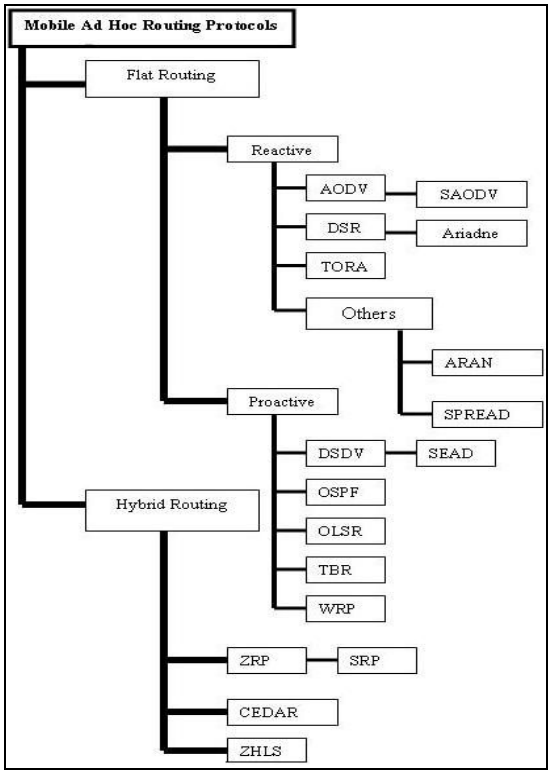

Fig. 1: Genealogy of Mobile Ad Hoc Routing Protocols

Figure 1 shows the three categories of Ad hoc RPs and various proposed Protocols under each category [1, 2, 15]. The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired. This is not the case, however, for on-demand routing protocols. When a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed [17]. In this paper we have presented a critical analysis of the above mentioned secure routing protocols. First we present a comparison between the two broad classes of routing protocols based on their routing methodology and other network parameters shown in Table 3.

3.1. Flat Routing Protocols

In a flat routing, the nodes communicate directly with each other. The problem with this is that it neither scales well nor allows for route aggregation of updates.

Proactive Protocols

Proactive protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. These protocols require each node to maintain one or more tables to store up to date routing information and to propagate updates throughout the network. As such, these protocols are often also referred to as table-driven. These protocols try and maintain valid routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronize the tables. Some examples of table driven ad hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) [14], Optimized Link State Routing Protocol (OLSR) [25] and Wireless Routing Protocol (WRP) [27]. These protocols differ in the number of routing related tables and how changes are broadcasted in the network structure.

Reactive Protocols

The major goal of on demand or reactive routing protocols is to minimize the network traffic overhead. These routing protocols are based on some type of "query-reply" dialog. They do not attempt to continuously maintain the up-to-date topology of the network. Rather, when the need arises, a reactive protocol invokes a procedure to find a route to the destination; such a procedure involves some sort of flooding the network with the route query. As such, such protocols are often also referred to as on demand. The common element in reactive protocols is the mechanism used for discovering routes. The source node emits a request message, requesting a route to the destination node. This message is flooded, i.e. relayed by all nodes in the network, until it reaches the destination. The path followed by the request message is recorded in the message, and returned to the sender by the

destination, or by intermediate nodes with sufficient topological information, in a reply message. Thus multiple reply messages may result, yielding multiple paths - of which the shortest is to be used. Some examples of source initiated ad hoc routing protocols include the Dynamic Source Routing Protocol (DSR) [12], Ad Hoc On-Demand Distance Vector Routing Protocol (AODV) [3], and Temporally-Ordered Routing Algorithm (TORA) [16]. No periodic updates are required for these protocols but routing information is only available when needed.

3.2 Hybrid Routing Protocols

These protocols try to incorporate various aspects of proactive and reactive routing protocols. They are generally used to provide hierarchical routing; routing in general can be either flat or hierarchical. The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption. Some examples of Hybrid Routing Protocols include CEDAR [28], ZRP [13] and SRP [1]. In what follows, we present a few of the proposed routing protocols from each class developed for the ad hoc networks. The most important protocols and those which dominate recent literature are AODV, DSR, SRP, ZRP, DSDV and TORA.

3.3 DSR

The distinguishing feature of Dynamic Source Routing (DSR) [12] is the use of source routing. DSR is a reactive protocol i.e. it doesn't use periodic updates. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. There are two basic parts of DSR protocol: route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes then it uses that path to transmit the packet. Also it attaches its source address on the packet. If there is no entry in the cache or the entry is expired, the sender broadcasts a route request packet to all its neighbors asking for a path to the destination. Until the route is discovered, the sender host waits. When the route request packet arrives to any other nodes, they check whether they know the destination asked. If they have route information, they send back a route reply packet to the destination. Otherwise they broadcast the same route request packet. Once the route is discovered, the sender will send its required packets using the discovered route as well as insert an entry in the cache for future use. Also the node keeps the age information of the entry to recognize whether the cache is fresh or not. When any intermediate node receives a data packet, it first sees whether the packet is sent to itself or not. If it is the destination, it receives that else it forwards the packet using the path attached on the packet.

3.4 ARIADNE

It is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig [6] based on DSR. It maintains authenticity on end-to-end basis, using symmetric key cryptography. It can authenticate routing messages using either shared secret keys, digital signatures or shared secrets in combination with broadcast authentication like TESLA. The Protocol enables the destinations to authenticate the Route Request sent by source node. The RREQ contains Message Authentication Certificate (MAC) which can be easily verified by the destination node. A per-hop hashing technique is used to verify that no node is missing from the node list [30]. Route maintenance is done using Distance Secure Routing (DSR) mechanism. However, Ariadne is very much immune to Worm Hole attacks through clock synchronization between nodes, but not in all situations.

3.5 AODV

Ad hoc On-demand Distance Vector (AODV) [3] is a combination of both DSR and DSDV. It follows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It uses destination sequence numbers to ensure loop

freedom at all times and by avoiding the Bellman-Ford "count-to-infinity" problem offers quick convergence when the ad hoc network topology changes. AODV finds routes only when required and hence is reactive in nature. The major vulnerabilities present in AODV protocols are: Deceptive increase of sequence number and Deceptive decrease of hop count. Zapata [2] applies security extensions to AODV using one-way hash functions to serve metric fields in Route Request (Route Discovery). He introduced Secure-AODV (SAODV) [29] where he suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation [33].

3.6 TORA

Temporarily ordered routing algorithm **(**TORA) is highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to provide better route aid for networks with dense, large population of nodes [33]. However to provide this feature TORA needs synchronization of the nodes which limits the application of the protocol. TORA is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when a link failure occurs. In comparison, all the other protocols need to re-initiate a route discovery when a link fails but TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has higher overhead for smaller networks.

3.7 DSDV

The Destination-Sequenced Distance-Vector (DSDV) [14] Routing protocol is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements such as making it loop-free. The distance vector routing is less robust than link state routing due to problems such as count to infinity and bouncing effect. In this, each device maintains a routing table containing entries for all the devices in the network. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbor devices. When a neighbor device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and re-computes the distance of the route which includes this link in the routing table.

3.8 SEAD

It is a Distance Vector Routing Protocol based on DSDV Ad Hoc Routing. It is a lightweight secure routing protocol presented by Hu, Johnson & Perrig [11]. The designers of Secure Efficient Ad Hoc Distance Vector Routing (SEAD) used efficient one-way Hash functions to provide authentication for both the sequence number and metric field in each routing entry. They avoid asymmetric cryptography to protect against DoS attack and to overcome limited CPU processing capability. The receiver of the achieved either through Message Authentication Certificate (MAC) or some broadcast authentication mechanism. It is too susceptible to Worm Hole attacks like SRP.

3.9 ZRP

The Zone Routing Protocol (ZRP) [31] is a hybrid routing protocol for mobile ad hoc networks which localizes the nodes into sub-networks (zones). It incorporates the merits of on-demand and proactive routing protocols. Within each zone, proactive routing is adapted to speed up communication among neighbors. The inter-zone communication uses on-demand routing to reduce unnecessary communication. The network is divided into routing zones according to distances between mobile nodes. Given a hop distance *d* and a node N, all nodes within hop distance at most *d* from N belong to the routing zone of N. Peripheral nodes of N are N's neighboring nodes in its routing zone which are exactly *d* hops away from N. An important issue of zone routing is to determine the size of the zone. An enhanced zone routing protocol, Independent Zone Routing (IZR), which allows adaptive and distributed reconfiguration of the optimized size of zone, is introduced in [32]. Furthermore, the adaptive nature of the IZR enhances the scalability of the ad hoc network.

3.10 SRP

Papadimitratos [1] proposed a Secure Routing Protocol (SRP) based on DSR. It is applied as an extension of a multitude of existing RPs such as DSR and ZRP. The protocol is proven robust against a se of attacks that attempt to compromise the route discovery. It provides the correct routing information regarding a pair of nodes provided they have prior security association. The source node initiates the route discovery by sending a Route Request (RREQ) packet (identified by a pair of identifiers, a query sequence number & a random query identifier) to the destination and replies are sent back strictly through the same route. SRP can only handle Black Hole attacks and not Worm Hole attacks. However, it can nevertheless prevent them.

4 Comparison of protocols

In this section we have presented a comparison between existing routing protocols. Table 4 compares the Proactive protocols and Table 5 compares the Reactive Protocols. The comparisons basically consider the characteristic properties of routing protocols in high load networks. The route updation column shows how the route tables are updated, and which nodes are sent the update messages. This influences the routing overhead. More the protocols are periodic and triggered more the overhead. The caching overhead changes according to the number of required routing tables and their sizes. The throughput is influenced by factors such as routing overhead and queue length. From Table 5 the routing overhead with DSR can be reduced by immediately sending request packets through the neighbors when no route exists. In high load conditions, DSR throughput is reduced as there is no metric for identifying stale routes, that may cause data packets to be dropped. Table 6 gives a comparison of some of the existing Hybrid Routing Protocols.

5 Summary

It is possible to construct some kind of suitability chart to be used for protocol evaluation shown in Figure 2.

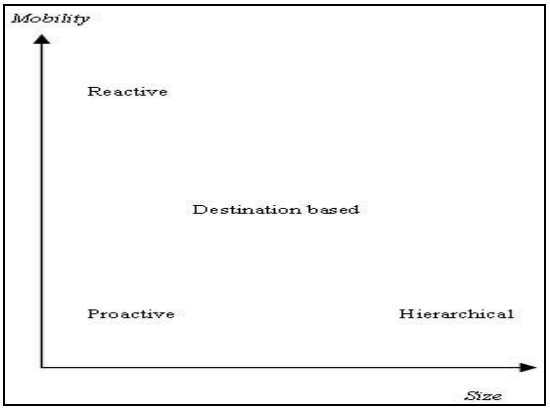

Fig. 2: Suitability Chart

The assumptions are as follows:

- The Proactive protocols have poorer performance characteristics with high mobility networks than reactive have. This is based on the fact that with high mobility it is not an easy task to manage consistent network information in all nodes.

- The Reactive Protocols have high performance provided that the network size is small enough.

- The Destination based protocols are assumed to scale a little bit better than Proactive Protocols because of smaller control traffic amounts.

- With very large size the hierarchical routing based Hybrid Protocols are very efficient, but these are hard to maintain while the network is in high mobile state.

6 Conclusions & Future work

6.1 Conclusions

In this paper we have presented the best known protocols for securing the routing function in mobile ad hoc networks and provided comparisons between them. Apart from this, there are still many challenges facing Mobile ad hoc networks. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. This is why Mobile Ad hoc Networks are becoming more and more prevalent in the world. The comparison we have presented between the routing protocols

indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing security solutions. Finally, we believe that more work is still required to justify the exact definition for secure ad hoc routing which will allow researchers to formally prove whether a proposed protocol satisfies all the security issues concerning Ad hoc Networks.

6.2 Future Work

As we have discussed in this paper, the research in the area of Routing Protocols over MANETs is far from comprehensive. Much of the effort so far has been on proposing Routing Protocols to support efficient and effective communications between nodes that form an ad hoc network. However, there exist many topics that deserve further research as discussed follows.

Scalability: There is a need to design a Routing Protocol that is scalable with respect to the number of nodes in the network and their mobility.
Security: Due to the inherent nature of ad hoc networks, security becomes more critical issue. Further investigation is needed to detect and catch the intruders from entering the network or stop the nodes from receiving information from intruder nodes.
Traffic: Investigation is required to efficiently control and distribute the network traffic between the nodes from source to destination because the traffic in most of the Routing Protocols is controlled by source nodes.
Power: The promiscuous nature of ad hoc networks is also a big issue for research as they consume a lot of power in broadcasting messages to achieve a high throughput.

Acknowledgements

The authors wish to thank the reviewers and editors for their valuable suggestions and expert comments that help improve the contents of paper.

References:

[1] P. Papadimitratos and Z.J. Haas. "Secure routing for mobile ad hoc networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[2] M. Zapata, N. Asokan, "Securing ad hoc routing protocols", WiSe'02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.

[3] C.E Perkins, E.M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[4] Patroklos G. Argyroudis And Donal O'mahony, University Of Dublin, Trinity College, "Secure Routing for Mobile Ad hoc Networks".

[5] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[6] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2002.

[7] H. Dang, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, 0163-6804, pp. 70-75, October 2002.

[8] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 1999.

[9] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[10] "Secure routing protocols for mobile ad-hoc wireless networks," in Advanced Wired and Wireless Networks, T.A.Wysocki, A.Dadej, and B. J. Wysocki, Eds. Springer, 2004.

[11] Y.C. Hu, D.B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," IEEE, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, 0-7695-1647-5, 2002.

[12] D.B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Ad Hoc Networking, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.

[13] Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of the Zone Routing Protocol", IEEE/ACM Transactions

on Networking, vol. 9, no. 4, pp. 427-438, Aug 2001.

[14] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers," Proc. ACM Conf. Communications Architectures and Protocols, London, UK, August 1994, pp. 234-244.

[15] Elizabeth M. Royer & Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks".

[16] P. Papadimitratos and Z.J. Haas. "Secure routing: Secure Data Transmission in Mobile Ad Hoc Networks", *Proc. ACM Wksp. Wireless Security 2003*, Sept. 2003, pp. 41-50.

[17] N.S. Yadav, and R.P.Yadav, 2007, Performance Comparison and Analysis of Table- Driven and On- Demand Routing Protocols for Mobile Ad-hoc Networks, International Journal of Information Technology, Vol.4, No. 2, pp 101-109.

[18] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communications Surveys & Tutorials, Vol. 10 No. 4, 4th Quarter 2008.

[19] C. E. Perkins, "Ad hoc Networking", Pearson Publication.

[20] Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security.

[21] F. Wang, B. Vetter, and S. Wu, "Secure Routing Protocols: Theory and Practice," Technical Report, North Carolina State University, May 1997.

[22] H. Li, Z. Chen, X. Qin, C. Li, H. Tan, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks," Technical Report, Department of Computer Science, University of Kentucky, Apr '02.

[23] N. Ahuja and A. Menon, "Security in Mobile Networks: Ad-hoc and Infrastructure," Computer and Information Sciences, University of Florida, Dec '01.

[24] M. Jakobsson, W. S, and Y. B, "Stealth Attacks on Ad-Hoc Wireless Networks," in *Proc. Vehicular Technology Conf., October, 6-9 2003*.

[25] T.H.Clausen et al., "The Optimized Link-State Routing Protocol. Evaluation through Experiments and Simulation", *Proc. IEEE Symp. Wireless Personal Mobile Communications* 2001, Sept. 2001.

[26] Y.Hu and D.B. Johnson, "Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks", *Proc. ACM SASN '04*, Oct 20,2004.

[27] S. Murthy, C. Siva Ram and B.S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, Chapter 7, 2004.

[28] A.A. Pirzada, C.McDonald and A. Datta, "Performance Comparison of trust-based Reactive Routing Protocols", *IEEE Trans. Mobile Computing*, vol. 5, issue 6, June 2006, pp. 695-710.

[29] Manel Guerrero Zapata. "Secure ad hoc on-demand distance vector (SAODV) routing". IETF MANET Mailing List, ftp://MANET.itd.nrl.navy.mil/pub/ MANET/2001-10.mail, October 8, 2001.

[30] G.V.S. Raju and Rehan Akbani, "Some Security Issues in Mobile Ad-hoc Networks," in proceedings of the Cutting Edge Wireless and IT Technologies Conference, November 2004.

[31] Z. J. Haas and M. R. Pearlman, .ZRP: a hybrid framework for routing in ad hoc networks,. pp. 221.253, 2001.

[32] P. Samar, M. R. Pearlman, and Z. J. Haas, .Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks,. in IEEE/ACM Transactions on Networking (TON), vol. 12, 2004, pp. 595.608.

[33] Anuj K. Gupta, Dr. Harsh Sadawarti, Dr. Anil K. Verma, "Performance analysis of AODV, DSR & TORA Routing Protocols", IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010.

[34] Anuj K. Gupta, Dr. Harsh Sadawarti, "Secure Routing Techniques for MANETs", International Journal of Computer Theory and Engineering (IJCTE), ISSN: 1793-8201, Article No. 74, Vol.1 No. 4, October 2009, pp. – 456-460.

Bibliography

Mr. Anuj K. Gupta is a research fellow in Punjab Technical University, Punjab, India. His research area is Mobile ad hoc networks, wireless networks & Data Communication. He has a teaching experience of around 10 years. Currently he is working as faculty in CSE Dept. at RIMT-IET, Punjab.
Email: seekanuj@gmail.com.

Dr. Harsh Sadawarti is Director at RIMT-IET, Punjab, India. He has a vast teaching and research experience of more than 20 years in the field of computer science. His areas of research are ad hoc networks, parallel computing & Distributed systems.
Email: harshsada@yahoo.com.

Dr. Anil K. Verma is faculty in Computer Sci. & Engg. Dept. at Thapar University, Patiala, Punjab, India. He has a vast teaching & research experience of more than 20 years. His areas of research are mobile ad hoc networks, wireless sensor networks & Network Security.
Email: akverma@thapar.edu.

Table 3: Comparison between Time-Driven & On-Demand Routing Protocols

Parameters	***Table-Driven (Proactive)***	***On-Demand (Reactive)***	***Hybrid***
Storage Requirements	Higher	Dependent on no. of routes maintained or needed	Depends on size of each zone or cluster
Route Availability	Always available	Computed as per need	Depends on location of destination
Periodic Route Updates	Required always	Not required	Used inside each zone
Delay	Low	High	Low for local destinations and high for interzone
Scalability	100 nodes	> 100	> 1000
Control Traffic	High	Low	Lower that other two types
Routing Information	Keep stored in table	Doesn't store	Depends on requirement
Routing Philosophy	Mostly flat	Flat	Hierarchical

Table 4: Comparison of Proactive Routing Protocols

Parameters	***DSDV***	***WRP***	***OLSR***
Route updation	Periodic, Triggered to the neighbors	Periodic, Triggered to the neighbors	Periodic, Triggered in the network
Loop free	Yes	Yes	Yes
Routing overhead	High	High	Low
Caching overhead	Medium	High	High
Throughput	Low	Low	Medium
Routing tables	2	4	4

Table 5: Comparison of Reactive Routing Protocols

Parameters	***AODV***	***DSR***	***TORA***
Route Creation	By source	By source	Locally
Periodic updation	No	No	No
Performance Metrics	Speed	Shortness	Speed
Routing overhead	High	High	High
Caching overhead	Low	High	Medium
Throughput	High	Low	Low
Multipath	No	Yes	Yes
Route updation	Non-periodic	Non-periodic	High routing overhead

Table 6: Comparison of Hybrid Routing Protocols

Parameters	***ZRP***	***ZHLS***	***DST***	***DDR***
Routing Structure	Flat	Hierarchical	Hierarchical	Hierarchical
Multiple routes	No	Yes	Yes	Yes
Beacons	Yes	No	No	Yes
Route information stored in	Intrazone & Interzone tables	Intrazone & Interzone tables	Route tables	Intrazone & Interzone tables
Route metric	Shortest path	Shortest path	Forwarding using the tree neighbors	Stable routing
Advantage	Reduced transmissions	Low control overhead	Reduced transmissions	No zone coordinator or zone map
Disadvantage	Overlapping zones	Static zone map required	Root node	Neighbors may become bottlenecks