A Comparative Study of various Secure Routing Protocols based on AODV

Dalip Kamboj
Department of Information Technology,
MMEC, Maharishi Markandeshwar University,
Mullana, Haryana, India

Pankaj Kumar Sehgal
Department of Information Technology,
MMEC, Maharishi Markandeshwar University,
Mullana, Haryana, India

Abstract— **The paper surveyed and compared various secure routing protocols for the mobile ad hoc networks (MANETs). MANETs are vulnerable to various security threats because of its dynamic topology and selfconfigurable nature. Security attacks on ad hoc network routing protocols disrupt network performance and reliability. The paper significantly based on base routing protocol AODV and Secure protocol based on AODV. The comparison between various secure routing protocols has been made on the basis of security services and security attacks. From the survey it is quite clear that these protocols are vulnerable to various routing attacks. A multifence secure routing protocol is still required to fulfill the basic security services and provide solution against various attacks.**

Keywords-ad hoc network; basic security servieces; security attack.

I. INTRODUCTION

Wireless networks have become increasingly popular in the past few decades, particularly with in the 1990's when they are being adapted to enable mobility and wireless devices became popular. Networks that support the ad hoc architecture are typically called wireless ad hoc networks or mobile ad hoc networks [1]. Such networks are typically assumed to be self-forming and selfhealing. This is because the typical applications of such networks require nodes to form networks quickly without any human intervention. Given the wireless links and mobility of nodes, it is possible that nodes may lose connectivity to some other nodes. This can happen if the nodes move out of each other's transmission range. As a result, it is possible for portions of the network to split from other portions of the network. In some applications it is also possible that some nodes may get completely disconnected from the other nodes, run out of battery, or be destroyed. For these reasons, nodes in a MANET cannot be configured to play any special role either in the way nodes communicate or in the way of providing communication services. This leads to a symmetric architecture where each node shares all the responsibilities. The network needs to be able to reconfigure itself quickly to deal with the disappearance (or reappearance) of any node and continue operating efficiently without any human intervention. Routing in such networks is particularly challenging because typical routing protocols do not operate efficiently in the presence of frequent movements, intermittent connectivity, network splits and joins. In typical routing protocols such events generate a large amount of overhead and require a significant amount of time to reach stability after some of those events.

Routing is an important function in any network [1], be it wired or wireless. The protocols designed for routing in these two types of networks, however, have completely different characteristics. Routing protocols for wired networks typically do not need to handle mobility of nodes within the system. These protocols also do not have to be designed so as to minimize the communication overhead, since wired networks typically have high bandwidths. Very importantly, the routing protocols in wireline networks can be assumed to execute on trusted entities, namely the routers. These characteristics change completely when considering ad hoc wireless networks. In ad hoc network the device will have to act a router as well. Ad hoc wireless network routing protocols [2] can be classified into the three major categories wiz table driven routing protocol, reactive or on-demand driven routing protocol and hybrid routing based on the routing information update mechanism. In the table driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains. For example DSDV [5], WRP [6], CGSR [7], STAR [8], OLSR [9], FSR [10], HSR [10] and GSR [11]. The Reactive or On-demand routing protocols do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routing information periodically. For example DSR [12], AODV [13], ABR [14], SSA [15], FORP [16], PLBR [17]. The Hybrid routing protocols combine the best features of the above two categories. Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For example CEDAR [18], ZRP [19] and ZHLS [20].

The above protocols do not provide any security mechanism against basic security services wiz authentication, confidentiality, integrity, authentication, non-repudiation and availability. These protocols are also vulnerable to various security attacks such as Rushing attack, Sybil attack, Black Hole attack, Wormhole attack, Blackmail attack, Replay attack and Routing table poisoning attack. Many protocols have been introduced to provide basic security services and mitigate against security attacks. For example SAODV [21], SAR [23], A-SAODV [24], MS-AODV [25], RAODV [26], TAODV [27], ISAODV [28] and SecAODV [29], SRPM [3], SecureAODV [4] and CBRP [22].

The rest of the paper explained as follow. The section II provides the information of the base routing protocol i.e. Ad hoc on demand distance vector routing protocol (AODV). The section III provides the information of secure routing protocol based on AODV. The section IV describes the comparisons based on basic security services. The section V describes the comparison on basis of various security attacks. The section VI describes the conclusion of this paper.

II. Ad-hoc On-demand Distance Vactor Routing (AODV)

AODV was an improvement on DSDV [5] because it typically minimizes the number of required broadcasts by creating routes on a demand basis. AODV [13] routing protocol uses reactive approach for finding routes, that is, a route is established only when it is required by any source node to transmit data packets. The protocol uses destination sequence numbers to identify the recent path. The source node and the intermediate nodes store the next node information corresponding to each data packet transmission. The source node floods the Route REQuest (RREQ) packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RREQ. A node updates its path information only if the destination sequence number of the current packet received is greater than the last destination sequence number stored at the node. A RREQ carries the destination identifier(DestID), the source identifier(SrcID), the source sequence number (SrcSeqNum) and destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum shows the freshness of the route that is selected by the source node. When an intermediate node receives a RREQ, it either forwards it or prepares a route reply (RREP) if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at packet. If a RREQ is received multiple times, which is indicated by BcastID-SrcID pair, then the duplicate copies are discarded. A timer is used to delete this entry in case a RREP is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of the data packets like DSR [12]. When a node receives a RREP packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop towards the destination.

III. Secure Routing Protocols based on AODV

Although there are several some routing protocol are based on AODV. Some are selected for survey and comparison for this paper. There are SAODV, A-SAODV, MS-AODV, RAODV, TAODV, ISAODV and SecAODV. The following subsections describe the protocols in detail.

A. *Secure Ad-hoc on demand distance vector Routing (SAODV)*

A secure version of AODV [13] called Secure AODV (SAODV). It provides features such as integrity, authentication, and nonrepudiation of routing data. It incorporates two schemes for securing AODV. The first scheme involves nodes signing the messages e.g. Route Request (RREQ), Route Reply (RREP). This allows other nodes to verify the originator of the message. This scheme can be used for protecting the portion of the information in the RREQ and RREP messages that does not change once these messages are created. However, RREQ and RREP messages also contain a field (namely the hop count) that needs to be changed by every node. Such mutable information is ignored by the creator of the message when signing the message. The second scheme of SAODV [21] is used for protecting such mutable information. This scheme leverages the idea of hash chains. Signing routing messages implies that the various nodes need to possess a key pair that makes use of an asymmetric cipher. In addition, nodes in the network also need to be aware of the authentic public keys of the other nodes.

B. *Security Aware Ad hoc Routing (SAR)*

SAR [23] protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. It uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are that it required excessive encrypting and decrypting at each hop during the path discovery. The discovered route may not be the shortest route in the terms of hop-count, but it is secure.

C. *Adaptive SAODV (A-SAODV)*

A-SAODV [24] optimizes the routing performance of secured protocols with help of a threshold mechanism. A-SAODV is a multithreaded application. In that protocol the cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other message and other thread to all other functions. Every node has queue of routing message to be signed or verify and the length of the queue implies the load state of the routing thread. Whenever a node processes a route request and has enough information to generate a RREP on behalf of destination, it first checks its routing message queue length. If the length of the queue is below a threshold then it reply otherwise, it forwards the RREQ without replying. The value of threshold can be changed during execution. The A-SAODV [24] also maintains a cache of latest signed and verified message in order to avoid signing and verifying the same message twice. This adaptive reply decision has a significant improvement on the performance of SAODV [21].

D. More Stable Ad-hoc On-demand Distance Vector Routing(MS-AODV)

MS-AODV [25] works according to existing AODV [13] in case of sending RREQ and REPLY packets. Packet formats are almost same. For measuring stability added some extra fields in the neighbor management table of the node and in the packets. In MS-AODV the forward path and reverse path setup are almost same as existing AODV [13] with a difference that Forward path setup is delayed. Each node stores its all neighbor's stability in Neighbor Management Table. Stability measurement is based on path stability which outperforms over all other parameters of stability measurement. Before sending data packet into the Reverse Path Setup, AODV [13] protocol discovers the routing path from source to destination. Source broadcasts RREQ packets to its neighbors and these packets are forwarded from node to node until the desired destination receives this packet. As the node forwards packets it updates its routing table as well as its stability table which is used for comparing stability of adjacent links. Thus several reverse paths are created from source to destination. Into the MS-AODV [25] the Forward Path Setup is different from existing AODV [13] protocol. In existing AODV, the destination sends REPLY packet as soon as it receives first RREQ packet. But in MS-AODV [25], as the destination needs to determine the most stable path, it needs to wait for a short while so that it can receive RREQ packet within this period as much as possible. RREQ packets arrive through multiple paths between source and destination. In each RREQ packet, the destination gets the cumulative stability of the path from the source to the destination. After comparing those values, the destination decides which path to be used for data communication and hence sends a REPLY packet to that path in reverse direction.

E. Reliable Ad-hoc On-demand Distance Vector Routing (RAODV)

The existing AODV [13] has been extended to RAODV [26] by adding two types of control packets: Reliable Route Discovery Unit (RRDU) and RRDU Reply (RRDU_REP). The RRDU messages are control packets sent by the source node along with RRDU-ID, to the destination at regular intervals and RRDU_REP message is the response of RRDU by the destination to the source node. RRDU_REP can only be generated by the destination. There is no impersonation i.e. no node other than the destination, can generate RRDU_REP on behalf of the destination. Reliability List (RL) field is also adding in the routing table entry. An entry in the RL has Source address, a field called Forward Data Packet Count (FDPC) and RRDU-ID, i.e. the triplet (Source address, FDPC, RRDU-ID). The Routing Table entry format of RAODV is same as that of AODV [13] except for the additional RL field. RAODV uses RREQ, RREP messages for route discovery and RERR, HELLO messages for route maintenance which is similar in AODV [13]. In addition, RAODV also uses RRDU and RRDU_REP to help discover the path and for reliability maintenance. In RAODV [26] the path discovery can be thought of as consisting of two phases. The phase I is same as AODV [13]. Whenever a node wishes to communicate with another node it looks for a route in its table. If a valid entry is found for the destination it uses that path else the node broadcasts the RREQ to its neighbors to locate the destination. The neighbor nodes again broadcast RREQ to their neighbors. The process continues until either the destination or an intermediate node with a fresh route to the destination is located. A reverse path is created for the source at each intermediate node. It must be noted that several reverse paths may be created in this process. The source receives RREPs from all these paths. But in AODV [13], it selects the one with minimum hop count and others are discarded. But in Phase II the source node sends an RRDU packet to all the nodes from which it gets the RREPs. Now since replies to RRDU, i.e. RRDU_REP packets are generated only by the destination and there is no impersonation, the source node will receive a unique RRDU_REP and the path discovery is completed.

F. Trusted Ad-hoc On-demand distance vector Routing (TAODV)

TAODV [27] is secure routing protocol which uses cryptography technologies recommended to take effect before nodes in the establish trust relationships among one another. The main salient feature of TAODV [27] is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time. TAODV (Trusted AODV) has several salient features: (1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them; (2) A node who performs malicious behaviors will eventually be detected and denied to the whole network. (3) The performance of the System is improved by avoiding requesting and verifying certificates at every routing step. That protocol greatly reduces the computation overheads. Assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures before the node performs routing behaviors. Some extra new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing with others. The main advantages of embedding trust model into the routing layer of MANET, save the consuming time without the trouble of maintaining expire time, valid state, etc. which is important in the situation of high node mobility and invalidity. Trusted AODV [27] are mainly three modules in the whole TAODV system: basic AODV [13] routing protocol, trust model, and trusted AODV routing protocol. Based on trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating.

G. Intrusion Detection Ad-hoc On-demand distance vector Routing (ISAODV)

The Intrusion Detection Systems (IDS) has been used for the support of secure Ad Hoc On Demand Distance Vector (AODV) routing, named IDS-based Secure AODV (IS-AODV [28]), in wireless ad hoc and vehicular network scenarios. The (IS-AODV) is based on the detection of behavior anomalies on behalf of neighbor hosts, with passive reactions, aiming to create a cluster whose route paths will include only safe nodes, eventually. That protocol is implemented by adopting an IDS solution and the concept of Statistically Unique and Cryptographically Verifiable (SUCV) identifiers, for IPv6-

based MANETs. IS-AODV [28] is based on SUCV and mutual verification of nodes behaviors during the path creation process. SUCV identifiers (or Crypto-based IDs, CBIDs) are used to realize a secure binding between IPv6 addresses and cryptography keys, without requiring any trusted Certification Authority (CA) or a Key Distribution Center (KDC). IS-AODV is different from SecAODV [29], because it uses the IDS as the basis for the implementation of secure AODV routing. In IS-AODV, in order to control the behavior of neighbors during the route discovery and data forwarding phases, each node monitors the traffic whose path includes the node itself: when a node N perceives a suspect behavior from a neighbor host, the IDS reaction is passive, that is, the information is not advertised to local nodes, and the node N does not rely/assist any suspect neighbor-node communication. In addition, unlike SecAODV [29], the ISAODV scheme does not require any cryptography operation in the intermediate nodes. The IS-AODV mechanism introduces a low-overhead additional field for standard AODV [13] Route Request (RREQ) and Route Reply (RREP) messages. A public key cryptography is used by end-nodes only (possibly replaced by more lightweight symmetric cryptography, after a safe path is found), to verify the signature of routing and data packets. This allows the end-to-end packet verification.

H. Secure AODV (SecAODV)

SecAODV and the snooping IDS complement each other in being able to detect most of the prevalent attacks. SecAODV [29] is a highly adaptive distributed algorithm designed for IPv6-based MANETs that does not require: (1) prior trust relations between pairs of nodes (e.g. a trusted third party or a distributed trust establishment), (2) time synchronization between nodes, or (3) prior shared keys or any other form of secure association. The protocol provides on-demand trust establishment among the nodes collaborating to detect malicious activities. A trust relationship is established based on a dynamic evaluation of the sender's "secure IP" and signed evidence, contained in the SecAODV [29] header. This routing protocol enables the source and destination nodes to establish a secure communication channel based on the concept of "Statistically Unique and Cryptographically Verifiable" (SUCV). The SecAODV implements two concepts.(1) Secure binding between IPv6 addresses and the RSA key generated by the nodes themselves, and independent of any trusted security service (2) Signed evidence produced by the originator of the message and signature verification by the destination, without any form of delegation of trust. The SecAODV protocol adds security features to the basic AODV [13] mechanisms, but is otherwise identical. A source node S that requests communication with another member of the MANET referred to as destination initiates the process by constructing and broadcasting a signed route request message RREQ. Upon successful verification, the node updates its routing table with S's address and the forwarding node's address. If the message is not addressed to it, it rebroadcasts the RREQ. When D receives the RREQ, it constructs a signed route reply message (RREP) addressed to then source node S, which includes the D's public key.

IV. COMPARISONS ON BASIC SECURITY SERVICESES

The table I provide a comparison on basic security services wiz Confidentiality, Integrity, Authentications, Nonrepudiation and Availability. The Confidentiality ensures that certain information is only readable or accessible by the authorized [30] party. Basically, it protects data from passive attacks. The principal of confidentiality specifies that only the sender and the recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access a message. The Integrity defines when the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of message is lost. Integrity [30] guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity [1] can apply to a stream of messages, a single message or selected fields within a message. The Authentication [30] ensures that the access and supply of data is done only by the authorized parties. Authentications mechanisms help establish proof of identities. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without authentication [1], an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes. The authentication process ensures that the origin of a electronic message or document is correctly identified. The Nonrepudiation are the situations [30] where a user sends a message and later on refuses that she had sent that message. Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver. Nonrepudiation is useful for detection and isolation of compromised nodes. The Availability defines the network resources should be available to authorized entities without excessive delays. The principle of the availability [1] states that resources should be available to authorized parties at all times. For example, due to the intentional actions of an unauthorized user C, and authorized user A may not be contact a server computer B. This would be defeat the principle of availability.

TABLE I. COMPARISON STUDY BASED ON BASIC SECURITY SERVICES

Performance Parameters type	**SAODV [21]**	**A-SAODV [24]**	**MS-AODV [25]**	**RAODV [26]**	**TAODV [27]**	**ISAODV [28]**	**SAR [23]**
Central trust authority	CA required	CA required	NOT required	NOT required	NOT required	NOT required	CA/KDC required
Authentication	Yes	Yes	No	Yes	Yes	Yes	Yes
Confidentiality	No	No	No	No	No	Yes	Yes
Integrity	Yes	Yes	No	Yes	Yes	Yes	Yes
Nonrepudiation	Yes	Yes	No	Yes	Yes	Yes	Yes
Availability	No	No	No	No	No	No	No

V. COMPARISONS ON BASIS OF VARIOUS SECURITY ATTACKS

The table II provides a comparison study based on various security attack wiz rushing attack, Sybil attack, black hole attack, wormhole attack, Blackmail attack, replay attack and Routing table poisoning. There are various types of attacks on ad hoc network which are describing following: In Rushing attack [1], the attacker simply forwards all control packets (but not data packets) received at one node (the attacker) to another node in the network. The rushing attacker may employ a wormhole to rush packets. This attack [2] impacts more on reactive routing protocol. The protocol defenses it by using randomized selection of route request message. Every node is expected to collect a threshold number of route requests. The Sybil attack assumed that every physical device has only one radio and device is incapable of simultaneously transmitting and receiving on more than one channel. The node allocates a channel to each of its neighbors to verify if any of its neighbors are Sybil [1] identities. The neighboring node is expected to transmit a message on the allocated channel. The verifier node then picks random channels for listening. If no message is heard on the channel selected then the corresponding node identity is assured to be a Sybil identity. In a Black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [31]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets. A Wormhole attack typically requires the presence of at least two colluding nodes in an ad hoc network. The malicious nodes need to be geographically separated in order for the attack to be effective. In this attack, a malicious node captures packets from one location and "tunnels" these packets to the other malicious node, which is assumed to be located at some distance. The second malicious node is then expected to replay the "tunneled" packets locally. The Blackmail attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [32]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated. A Replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties. Unless mitigated, the computers subject to the attack process the stream as legitimate messages, resulting in a range of bad consequences, such as redundant orders of an item. Routing table poisoning attack is classified as internal attack, as selfish node or set of misbehaving node implement this attack for purpose to save the batterylife or exploit the routing.

TABLE II. COMPARISON STUDY BASE ON VARIOUS SECURITY ATTACKS

Security Attack	**SAODV [21]**	**A-SAODV [24]**	**MS-AODV [25]**	**RAODV [26]**	**TAODV [27]**	**ISAODV [28]**	**SecAODV [29]**	**SAR [23]**
Black-Hole	No	No	No	Yes	No	No	No	No
Wormhole	No	No	No	Yes	No	No	No	No
Blackmail	NA	NA	NA	NA	NA	NA	NA	NA
Denial of Services	No	No	No	No	No	No	No	No
Replay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rushing attacks	No	No	No	Yes	No	No	No	No
Routing table poisoning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

VI. CONCLUSION

Secure Routing is one of the most basic and important tasks in MANETs. This paper reviewed various secure routing protocols based on AODV. From the comparative studies it is quite clear that these protocols are vulnerable to various routing attacks.

It has been observed none of secure routing protocol provides the availability service. Two protocols ISAODV and SAR provide the Confidentiality, Integrity, Authentications, Nonrepudiation. Only one protocol MSAODV does not provide any basic security services.

All the secure protocols provides the protection against replay and routing table poisoning attack but does not provide the protection against black-hole attack, blackmail attack, rushing attack and DoS. Only RAODV provides the protection against black-hole attack, wormhole attack, rushing attack.

In nutshell, there is no single mechanism which can provide basic security services and protection against various security attacks. So, there is a requirement of a multifence mechanism which can provide basic security services as well mitigate against various security attacks.

REFERENCES

[1] Farooq anjum and Petros Mouchtaris, "Security for wireless ad hoc networks," John Wily, 2007.

[2] C.Siva Ram Murthy and B. S. Manoj, "Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, ISBN 013147023X, May 2004.

[3] S. Khan and K.K. Loo, "SRPM Analysis in the Presence of Sinkhole attack in Hybrid Wireless Mesh Networks," In International Journal of Research and Reviews in Ad Hoc Networks Vol. 1, No. 1, March 2011.

[4] Suman Deswal and Sukhbir Singh, "Implementation of Routing Security Aspects in AODV," In International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[5] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-vector-Routing (DSDV) for Mobile Computers,” SIGCOMM, UK, pages 234-244, 1994.

[6] S. Murthy and J.J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Network”, In ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, vol. 1, no. 2, pages 183-197, October 1996.

[7] C. C. Chiang, H. K. Wu, W. Liu, and M. Gerla, “Routing in Clustered Multi-Hop Mobile Wireless Netwroks with Fading Channel,” Proceedings of IEEE SICON 1997, pp. 197-211, April 1997.

[8] J.J. Garcia-Luna-Aceves and M. Spohn, “Source-Tree Routing in Wireless Networks,” Proceedings of IEEE ICNP, Pages 273-282, October 1999.

[9] T. Clausen and P. Jacquet, eds, “Optimized Link State Routing Protocol (OLSR),” IETF RFC 3626, October 2003.

[10] A. Iwata, C. C. Chaing, G. Pei. M. Gerla, and T.W. Chen, “Scalable Routing Strategies for Ad Hoc Wireless Networks,“ In IEEE Journal on Selected Areas in Communications, vol. 17. no. 8, pp. 1369-1379, Augest 1999.

[11] T.W. Chen and M.Gerla, “Global state Routing: A New Routing Scheme for Ad Hoc Wireless Networks,“ Proceeding of IEEE ICC 1998, pp. 171-175, June 1998.

[12] D. Johnson and D. Maltz., “Dynamic source routing in ad-hoc wireless networks routing protocols,” In Mobile Computing, pages 153-181. Kluwer Academic Publishers, 1996.

[13] C.E.Perkins and E.M.Royer, “Ad hoc On-Demand Distance Vector Routing,” Proc. 2nd IEEE Workshop of Mobile Comp. Sys. and Apps., pages 90-100, Feb. 1999.

[14] C.-K. Toh., “Associativity-based routing for ad-hoc mobile networks,” WirelessPersonal Communications, 4(2):103-139, 1997.

[15] R.Dube, C.D.Rais, K.Y. Wang and S.K. Tripathi, “Signal Stability-Based Adaptive Routing for Ad Hoc Mobile Networks,” IEEE Personal Communications Magazine, Pages 36-45, February 1997.

[16] W. Su and M.Gerla, “IPv6 Flow Handoff in Ad Hoc Wirless Networks Using Mobility Prediction,” Proceeding of IEEE GLOBECOM, Pages 271-275, December 1999.

[17] R.S. Sisodia, B.S. Manoj, and C. Siva Ram Murthy, “A Preferred Link-Based Routing Protocol for Ad Hoc Wireless Networks,” In Journal of Communication and Networks, vol. 4, no. 1, pp. 14-21, March 2002.

[18] P. Sinha, R. SivaKumar, and V. Bharghavan, “CEDAR : A Core Extraction Distributed Ad Hoc Routing Algorthm,” In IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1454-1466, Augest 1999.

[19] Z. J. Haas, “The Routing Algorithem for the Reconfigurable Wireless Networks, ” Proceedings of ICUPC 1997, vol. 2. pp. 562-566, October 1997.

[20] 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, Augest 1999.

[21] Manel Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector (SAODV) Routing,” draft-guerrero-manet-saodv-06.txt, September 5, 2006.

[22] Seyed Amin Hosseini Seno, Rahmat Budiarto andTat-CheeWan, ”A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority,” In King Fahd University of Petroleum and Minerals 2010, 15 January 2011.

[23] R. Kravets, S. Yi, and P. Naldurg, ”A Security-Aware Routing Protocol for Wireless Ad Hoc Networks,” In ACM Symp. On Mobile Ad Hoc Networking and Computing, 2001.

[24] R Alekha Kumar Mishra and Bibhu Dutta Sahoo, “A Modified Adaptive-Saodv Prototype For Performance Enhancement In Manet,” In International Journal Of Computer Applications In Engineering, Technology And Sciences (Ij-Ca-Ets), Volume 1 : Issue 2 , Page: 443, April ’09 – September ’09.

[25] Tamanna Afroze, Saikat Sarkar, Aminul Islam and Asikur Rahman, ” More Stable Ad-hoc On-Demand Distance Vector Routing Protocol,” In 978–1–4244–2800–7/09/$25.00 ©2009 IEEE.

[26] Sandhya Khurana, Neelima Gupta and Nagender Aneja, ”Reliable Ad-hoc On-demand Distance Vector Routing Protocol,” In Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL’06) 0-7695-2552-0/06 $20.00 © 2006 IEEE.

[27] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, ”A Trust Model Based Routing Protocol for Secure Ad Hoc Networks,” In IEEEAC, 0-7803-8155-6 © 2004 IEEE.

[28] Luciano Bononi and Carlo Tacconi, “Intrusion detection for secure clustering and routing in Mobile Multi-hopWireless Networks,” In © Springer-Verlag Published online: 10 July 2007.

[29] Anand Patwardhan , Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis, “Secure Routing and Intrusion Detection in Ad Hoc Networks,” To appear in the Proceedings of the 3rd International Conference on Pervasive Computing and Communications(PerCom 2005), Kauai Island, Hawaii, 2005.

[30] Atul Kahate, Cryptography and Network Security, Tata Mcgraw Hill Education private Limited, 2008.

[31] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACMSE’04, April 2-3, 2004, Huntsville, AL, USA.

[32] Patroklos g. Argyroudis and donal o’mahony, “Secure Routing for Mobile Ad hoc Networks,” IEEE Communications Surveys & Tutorials Third Quarter 2005.