Secure Routing Protocol base on secure path in ad hoc wireless networks

Saud Al otaibi, Francois Siewe
Software Technology Research Laboratory , De Montfort University, Leicester, UK,
binrogeish@hotmail.comfsiewe00@dmu.ac.uk

ABSTRACT: ***Ad hoc wireless networking is a new approach to wireless communication with potential applications in very unpredictable and dynamic environments. Many applications today, especially in military and emergency situations, are based upon ad hoc wireless networks. The security requirements of these networks are harder to enforce than in a traditional network. Securing the routing in ad hoc wireless networks creates difficulties that do not exist in traditional networks. These networks have neither centrally administrated secure routers nor strict policies of use. In this paper, we present a new secure routing protocol, in order to protect the network against any malicious attack and to satisfy our requirements, based on secure path node-to-node routing.***

KEYWORDS: ***Ad hoc wireless network, EHARP, SEHARP***

I. INTRODUCTION

The nodes in ad hoc wireless networks act both as regular terminals (source or destination) and as routers for other nodes in the network, unlike fixed wired networks, such as the Internet, where dedicated routers are controlled by a service provider. The provision of security becomes a challenging task in these networks, owing to the absence of dedicated routers. The task of ensuring secure communication in ad hoc wireless networks is difficult for reasons including the mobility of nodes, limited processing power and limited availability of resources, such as battery power and bandwidth.

The network topology will change rapidly, because nodes in the networks are highly mobile, thus forming and breaking links. Therefore, routing in ad hoc wireless networks is an especially hard task to accomplish securely, robustly and efficiently at the same time. Security requirements such authentication, non-repudiation, data integrity and confidentiality, which would otherwise be provided by a central server, must be enabled and provided by all nodes in such a network.

Ad hoc wireless networks rely on the collaboration of the nodes involved for the network to create itself and operate efficiently. While maintaining suitable routing information in a distributed way is a challenging issue in such networks, it is even more challenging to secure the protocols used for routing [5]. At the network level, an ad hoc network fundamentally requires secure routing protocols, as these enable a communication path to be established. On the other hand, most of the routing protocols [3, 4,] designed for these networks have no consideration for security, operating with an implicit assumption of trust among the nodes. This provides opportunities for malicious attackers intent on bringing down the network. Many types of routing protocol exist and have been extensively researched, with a view to finding solutions to security vulnerabilities.

In fact, none of these approaches is designed to satisfy all requirements of a secure routing protocol [6, 7, 8, 9, 10]. In order to defend against attacks, the security mechanisms should be able to protect network management information and any other susceptible information. Moreover, the design of security mechanisms should fulfil the requirements of secures routing, which are:

- Confidentiality: ensures that only authorised users can access or reveal transmitted messages.
- Integrity: ensures that unauthorised persons cannot modify, alter or retransmit data to another destination.
- Authentication: ensures that both end-peers are who they claim to be.
- Non-repudiation: ensures that the sender/receiver cannot deny sending/ receiving.
- Guarantee of correct route discovery: ensures that the protocol is able to find the route and establish the correctness of the selected route

978-0-7695-3930-0/09 $26.00 © 2009 IEEE
DOI 10.1109/IFCSTA.2009.133

IEEE computer society

- Stability against attacks: ensures that the protocol is able to revert to its normal operation after any attack.
- Availability: ensures that resources and entities are available when needed by the intended parties.

None of these approaches guarantees the correct route discovery. Each detects or prevents one or more types of attack and most are extensions of existing protocols but do not solve the problems of these protocols, such as overheads and effective mobility.

Our contribution is to design a secure enhanced direction heading angle routing protocol (SEHARP) for ad hoc networks based on the integration of security mechanisms that could be applied to the EHARP routing protocol. It proposes a novel secure routing protocol to improve the security level in ad hoc networks, based on key management and a secure path, which protects data to satisfy our security requirements. This paper is organized as follows: in Section 2, we will illustrate the related work in ad hoc wireless networks; Section 3 explains our security requirements; in Section 4 we propose an approach to introduce a new routing protocol in ad hoc wireless networks; and Section 5 concludes the paper.

II. RELATED WORK

A. Routing protocol of ad hoc wireless networks

In an ad hoc wireless network, each node works as a host as well as a router and will propagate packets for other nodes in the network which are not within direct wireless broadcast range of one another. Every node participates in the network administration and routing schema, owing to the constantly changing network topology. According to routing protocols, each node can discover multiple-hop paths through the network to any other node. Many different routing protocols, such as Destination Sequenced Distance-Vector (DSDV) [8], Ad hoc On-demand Distance Vector (AODV) [9] and Dynamic Source Routing (DSR) [10] protocols have been developed for an ad hoc wireless network.

These can generally be classified according to the routing information update mechanism into three categories: proactive, on-demand and hybrid. Proactive protocols, also known as table-driven protocols, require every node to maintain one or more tables in order to store the network topology and routing information. This information is updated frequently by exchanging routing information; thus the periodic updating of existing routing information is essential. Unlike proactive routing protocols, reactive ones, also known as on-demand protocols because they establish routes when required by using a route discovery process and source, do not maintain the network topology information and route to each destination of the network. Hybrid protocols combine the features of reactive and proactive types in order to offer routing solutions, adapting them to suit the specific conditions, thus generally providing the most advantageous option.

B. Securing routing protocol in an ad hoc wireless network

Ad hoc wireless networks have some weaknesses such as lack of infrastructure, limited computation, decentralization and susceptibility to tampering; thus they suffer some critical security problems. In particular, the operation depends on the assumption of the routing protocol functioning generally [1, 2].

Attacks on ad hoc wireless networks [2] can be divided into two groups, namely passive and active attacks. A passive attack, where the attackers try to eavesdrop on the data or the network traffic without altering it, does not disrupt the operation of the network; but the requirement of confidentiality is violated if an adversary is able to interpret the data gathered through snooping. This type of attack is less harmful than an active one, yet is much harder to discover, because the attacker does not interfere with the operation. One way of overcoming such problems is to use powerful mechanisms to encrypt the data being transmitted, thus making it unlikely for eavesdroppers to obtain any useful information from the data overheard.

In active attacks, the attackers actively alter, modify or abstract data; by changing or destroying the data being exchanged in the network, they disrupt its normal functioning. Active attacks can be classified further into two categories, external and internal. External attacks are caused by nodes that do not belong to the network, while internal ones are from compromised nodes that belong to the network. Since the adversaries are already part of the network as authorised nodes, internal attacks are more severe and difficult to detect than external ones.

Some types of active attack, including wormhole, routing table overflow, black hole, impersonation and information disclosure, can be launched against an ad hoc wireless network layer and may affect the operation of the network.

Several secure routing protocols such as SAR [12], which uses security as one of the key metrics to find the path of routing, and SEAD [15] have been proposed for ad hoc wireless

networks. These reduce the overheads and speed up the routing process, since they use efficient one-way hash functions, RSA [11]. The essential idea of the proactive RSA is that it uses distributed shared keys, ARAN [13]. It is dependent on the use of cryptographic certificates, Secure AODV [14]. It uses schemes such as digital signatures and is dependent on source and end-to-end authentication.

III. Our Security Requirements

The following security requirements are to be satisfied by SEHARP.

- Detection of malicious nodes: If there are malicious nodes in a network, then the secure routing protocol should be able to detect them and avoid choosing such nodes during the routing process.
- Authentication: It is fundamental to verify the identity of an ad hoc network node and its fitness to access the network. In other words, ad hoc network nodes that wish to communicate with each other must ensure that they are communicating with the right party and that they are genuine, not impersonators. They must ensure that data is from the origin and not modified or falsified.
- Authorisation: The nodes in ad hoc networks need to have accurate authorisation in order to access shared resources on the network. This ensures that only authorized nodes are allowed to enter the network, store information and use the information on their devices. In addition, Role-Based Access Control (RBAC) provides different priority levels, to guarantee that network elements and individuals can only gain access to and perform operations on stored information, resources, services and applications.
- Confidentiality: The information that is sent between the ad hoc network nodes resident on their devices, or related to their locations, needs to be protected. This is to ensure that the data which has been sent between the ad hoc network nodes is the same and has not been modified, deleted or retransmitted to another node or entity.
- Availability: The availability of a network means that its essential services and applications should be accessible at any time when they are needed, even in the event of a breach in security. This availability ensures the survivability of the network, despite malicious attacks (denial of service), or the misbehaviour of particular nodes. This requirement is especially important in ad hoc networks, where security breaches, attacks and malfunctions are more frequent and less likely to be detectable.
- Data integrity: The information that is exchanged between the ad hoc network nodes needs to be protected in order to ensure that messages which have been sent are the same, and have not been modified, deleted or retransmitted to another node or entity. This is most fundamental in situations such as banking, military operations and equipment controls (e.g. trains or planes) where such modification or deletion could cause potential damage.
- Non-repudiation: This ensures that any ad hoc network node which sends/receives a message, or initiates a 'not deny' on receiving/sending packets to/from other nodes, is genuine and proves who the sender is. This is very important in situations of dispute or disagreement over events. This can be achieved using techniques such as digital signatures that relate the data or action to a signer.
- Guarantee of secure correct route discovery: This ensures that the protocol is able to find the route correctly and ensure the security of the selected route.

IV. Our approach

Our main focuses are to introduce SEHARP to protect data transmission and to form a secure routing protocol. The network consists of a group of mutually trusting nodes. There are two types of node, which are:

User Node (UN): Normal ground nodes, typically soldiers.

Network Back-Bone Node (NBBN): Usually units or master nodes located within the network, for example tanks. NBBNs can establish direct wireless links for communication amid themselves, as shown in Figure 1.

The network based on NBBNs is responsible for the key certificates and manages them. There are four NBBNs in each network, because a defining characteristic of EHARP is that there should be four head directions so that each has an NBBN. Our approach locates four NBBNs to achieve our requirement for availability and non-repudiation.

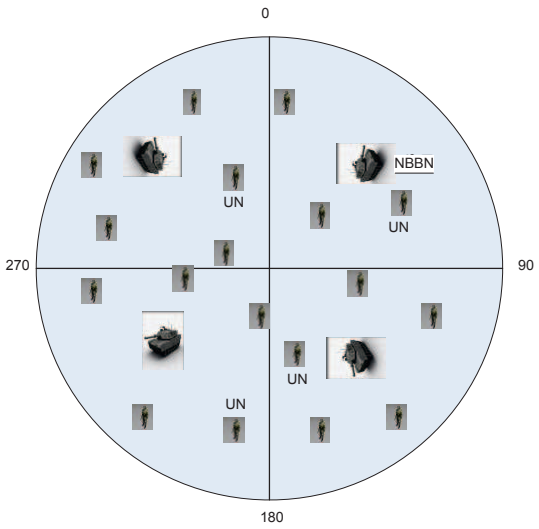


Figure 1. User nodes and network backbone nodes in a network

All user nodes should be able to carry out the encryption algorithms with limited computational power. All UNs in the network should trust any data message or any message signed using the corresponding private key.

Each user node has enough memory to store information such as the public keys and certificates of many other nodes.

SEHARP works as a group and has three stages:

- Distribution keys and certificate stage.
- Secure path stage.
- Secure routing protocol stage.

A. Distribution keys and certificate stage

Our scheme adopts the NBBN because of its superiority in distributing keys and achieving integrity and non-repudiation. The system uses private and public keys. The private key is used to sign the certificate and the public key of all the nodes, while the public key is used to renew certificates that are issued by another NBBN.

All nodes must have a copy of the NBBN's own public key to verify signatures. The public keys and the corresponding private keys of all nodes are created by the NBBNs, which also issue the public-key certificates of all nodes.

Each node has its own public/ private key pair. Public keys can be distributed to another node in the secure path stage, while private keys should be kept confidential to individual nodes. The NBBN signs the public key certificate for all nodes, so that these signings take place offline before the nodes can enter the network.

Each node in our approach receives exactly one certificate after securely authenticating its identity to the NBBN.

Each node will hold its digital certificate in a Node DataBase (NDB). The main structure of node digital certificates contains the identifier of the node, its public key, the name of the NBBN issuing this certificate, the certificate issue and expiry dates, and the public key of the NBBN. Finally, the contents of the certificate will be attached to the digital signature of the NBBN.

All nodes in a network should maintain fresh certificates with the NBBN. In the secure path stage, nodes use their certificates to authenticate themselves to other nodes in the network.

B. Secure Path Stage Node-to-Node

Our approach is to use a public-key algorithm to establish secure paths between nodes. The secure path stage (SPS), based on all nodes, should have a secure path with other nodes before sending any route request packet (RRP). Any node receiving an RRP from the source node or another node without a secure path should discard the request. In our approach, each node is given the system public key in order for any nodes to be able to send a secure path request (SPR) to another node the first time the certified public keys are exchanged. The authenticity of the certificate can be confirmed as the nodes have the system public key. The first objective of the SPS is the exchange of the certified public keys and their confirmation, while its second objective is to ensure the identity of the sender before acceptance of the RRP. The SPS considers secure authentications node by node.

1) *Source node*

When the source node S has an RRP for node D, it looks for it in its route table, then acts as follows, depending on whether it finds it.

A) If it finds it:

- S will send an SPR specifying the type of packet (SPR), the IP address of the destination (IPD), S's certificate (certS), all signed with S's private key.
- Destination node D will verify the signature and certS.
- If the signature and certS are validated, then D will send a reply to send the secure path request (RSPR) that it contains, as shown in Figure 2.

This will specify the type of packet (RSPR), the IP address of the source (IPS), D's certificate (certD), all signed with D's private key, and it will save certS in its NDB. Otherwise, the destination node D will discard the request.

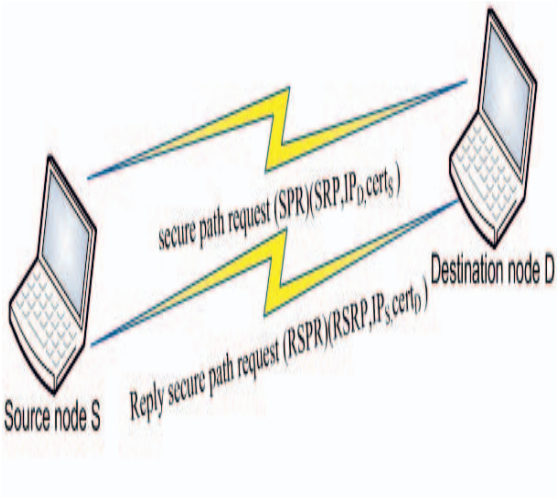


Figure 2. Secure path request and reply between S node and D node.

B) Otherwise:

- Source node S will send an SPR to a neighbouring (intermediate) node specifying the type of packet (SPR), IPD and certS, all signed with S's private key.

Intermediate node

- The intermediate node I will verify the signature and certS.
- If these are validated, then D will send an RSPR specifying the type of packet (SPR), the IP address of the source (IPs) and I's certificate (certI), all signed with I's private key, as shown in Figure 3.

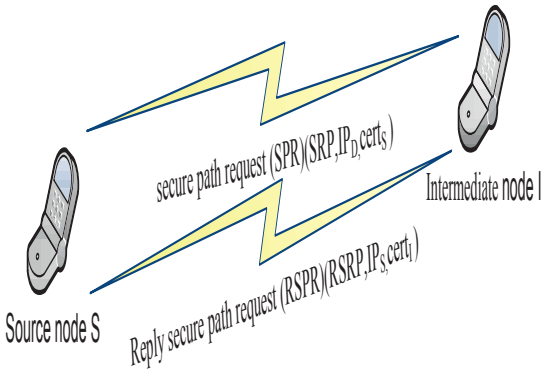


Figure 3. Secure path request and reply between S node and I node.

- To make a secure path with its neighbour, node I will send an SPR to a neighbouring node specifying the type of packet (SPR), IPD and certI, all signed with I's private key, as show in Figure 4.

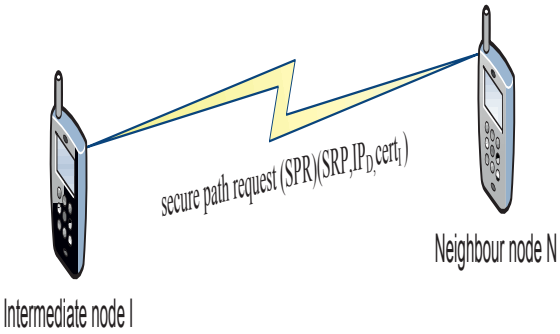


Figure 4. Secure path request from intermediate node

C) Secure routing protocol stage

At this stage our approach uses a hybrid of security mechanisms to introduce SEHARP so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route.

The security mechanisms that the protocol uses are the hash function, digital signature, time synchronisation and route discovery request, each of which is now explained in turn.

1) Hash function

Function

A hash function is used to encrypt and update the data necessary for the routing process in order to secure the mutable data, which in this case is the head direction and time to find a destination whose information uses hash chains.

Description

- Our protocol (SEHARP) uses hash chains in order to secure the mutable data of the head direction and td, the maximum time to find a destination node, for all nodes in the network, including an intermediate node and destination node, which when it receives the message can verify that the mutable data has not been decremented by any attacker.

SEHARP forms a hash chain by applying it one way.

- A hash function is the operation whereby a node creates an RREQ or RREP.a hash function repeatedly to begin.

The setting of the hash function is as follows:-

1) Assign a random number at the beginning and as the beginning value

- This sets the Hash field to Hash = beginning.

2) Set MaxHashCount field to the TD time to find destination value from the IP header.

- MaxHashCount = Time to Find Destination.

3) The Hash_Function field is set to indicate which hash function is employed. Hash_Function = h

4) Calculate Top_Hash by hashing beginning value as_hash_Count times.

- Top_Hash = h MaxHashCount – h hash_Count
- hash count = time to find neighbour
- where h is a hash function and h j (y) is the result of applying the function h to y j times

When a node is retransmitted an RREQ or an RREP message is used to verify the hash count. The node performs the following operations:-

1) It applies the hash function indicated by Hash_Function field by MaxHashCount minus hash Count times to the beginning value in the Hash field and verifies that the value is equal to the value contained in the Top_Hash field. Top_Hash = h MaxHashCount – h Hash_Count.

2. Before rebroadcasting an RREQ or forwarding a RREP, a node uses the hash function from the Hash value for the new node Hash = h (Hash).

2) Digital Signature

Function

The signature is used to protect the non-mutable data, which is data not required or changed in the routing process. Digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation.

Description

- SEHARP has two digital signatures. The first one is the source signature used to protect the integrity of the non-mutable data in RREQ and RREP messages, which means that the source signs everything. The second is the node-by-node signature, based on who obtained a secure path, and every intermediate node afterwards verifies the hash function, updates information and provides a signature for the updating. When a node receives an RREQ, it first verifies the signature of the owner and of the secure path before creating or updating a route to that neighbour. Only if the signature is verified will it update a route and set td to find the neighbour. After it is updated, it will sign all new updating and fields node by node from the RREQ. In the event of a failure, it will discard the RREQ. The destination node, when it receives an RREQ, first verifies the signature of the source and the signature of the intermediate node that has a secure path by field signature node-to-node. In the event of a failure, then the RREQ will be discarded.

3) Time synchronisation

Function

A timestamp is used to protect the route path from specific attacks.

Description

- The EHARP protocol is based on the time to find the destination and neighbouring nodes. When a node has a request packet, it calculates the time to find a neighbour and destination, and after creating the packet uses the timestamp; then the node

that has received the packet must verify it from the timestamp.

4) Route Discovery Request

A) Source node

To secure routing, the EHARP protocol has an additional secure suffix on the original message format to carry out the expansion; its format is shown in Table I.

Table I. SECURE SUFFIX MESSAGE FORMAT

TYPE	Length	Hash Function	Max Hash Count
Top Hash			
Source Signature			
Timestamp			
Node-to-Node Signature			
Hash			

In the table, the type of suffix field for a secure RREQ message has a value of 32, while for an RREP message the value is 33. The suffix is lengthened for security in addition to Type and lengthening of the number of bytes outside the field. Hash Function chosen field, said hash function, algorithm chosen is the value randomly, at present only to support the function. MaxHashCount field values from the source node in the routing message are sent when randomly assigned, When these four fields are accounted for by a byte store, TopHash field value equal to the field MaxHashCount designated by the hash function to do the hash calculation, MaxHashCount times the value of storage space size is 20 bytes.

When the source node sends a route request packet, SEHARP sets the max hash count field equal to the time to find the destination node (TD) field from the IP header; assigns a random number and sets the hash field equal to it; and applies the hash function specified by the corresponding field max hash count multiplied by the random number, storing the calculated result to the top hash field. Moreover, the source node digitally signs all fields of the SEHARP packet (except the HopCount domain) and the field before the global suffix of the message. Node-to-node Signature intermediate node on the information stored signature, in RREQ source node signature information, including SEHARP packet (except HopCount domain) and the suffix field before the security message. Before signature the source node uses a timestamp.

B) Intermediate node

The signature line in the route discovery and route maintenance process occurs before sending the routing information and before the beginning of the calculation. Intermediate nodes, on receipt of an RREQ message, require secure authentication to activate. The process involves four steps:

1) The TopHash value field is verified by comparing the rustle of the Hash function and so on (MaxHashCount-hashCount) times the same hash result;

2) Verification of the signature of the source node;

3) Verification that the signature on the node-to node is the owner's secure path;

4) Verification of the timestamp. In the event of a failure the message is discarded. The intermediate node, before forwarding messages to its neighbours, will re-sign carefully and be used to replace the value of the security suffix node-to-node. The signature field must also be updated before the Hash value, and its value will be equivalent to the original to provide a value for computing Hash.

C) Route Reply

Destination node

When the destination node D has received the route request packet, it will verify three steps, i.e. hash function, signatures and timestamp, and if all these are valid, it will update the information, set the hash function and sign all information. The destination node will sign only in the node-to-node signature field and send the message along the reversed path in the network, which is determined by the nodes recorded.

Intermediate node

If an intermediate node receives a route request message, it will check the security and if all steps are valid it will accept the message; otherwise it will discard it. When it has information about the destination node stored in its cache table (a valid path to the destination), then the intermediate node will update and add its information. It will calculate and set the hash function and sign all updated information, then sign in the node-to-node field and send the message along the reversed path in the network, which is determined by the nodes recorded.

V. CONCLUSION

In this paper, we have presented a secure routing protocol based on key management, a secure path, and protecting data to satisfy our security requirements. After understanding security requirements and identifying the types of attack the network might face, we proposed the security mechanism most suitable to satisfy those security requirements, having the following elements:

asymmetric encryption (used to protect non-mutable data).

hash function (used to protect mutable data)

time synchronisation.

All these mechanisms when applied to routing protocols should prevent external attacks, including black holes and routing holes, while providing viability, confidentiality and authentication. Time synchronization is used to provide the protocol with the ability to find the route and to ensure that the selected route is the correct path. The digital signature mechanism, when applied to routing protocols, should prevent internal attacks, including impersonation, and should also provide non-reputation and integrity.

REFERENCES

[1] C.-K. Toh, , "Ad hoc Mobile Wireless Networks: Protocols and Systems", Prentice- Hall, New Jersey, pp: 34-37, 2002

[2] C. Siva Ram Murthy and B.S. Manjo, "Ad hoc Wireless Networks: Architectures and Protocols", Prentice Hall communications engineering and emerging technologies series Upper Saddle River, 2004.

[3] Singh S., Raghavendra C.S., "Power efficient MAC protocol for multihop radio networks", Personal, Indoor and Mobile Radio Communications, 1998. The Ninth IEEE International Symposium on, Volume: 1 , 8-11 Sept. 1998, pp:153 – 157.

[4] Perkins C.E., Royer E.M., "Ad-hoc on-demand distance vector routing Mobile Computing Systems and Applications", Proceedings. WMCSA'99. Second IEEE Workshop on, 25-26 Feb. 1999, pp: 90 – 100.

[5] Ching-Chuan Chiang, Gerla M., Zhang L., "Adaptive shared tree multicast in mobile wireless networks", Global Telecommunications Conference, GLOBECOM 98. The Bridge to Global Integration. IEEE , Volume: 3 , 8-12 Nov. 1998, pp:1817 – 1822.

[6] Toh, C.-K., "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks", Communications Magazine, IEEE, Volume: 39 , Issue: 6, June 2001, pp:138 – 147.

[7] Holland G., Vaidya N., "Impact of routing and link layers on TCP performance in mobile ad hoc networks", Wireless Communications and Networking Conference, WCNC. 1999 IEEE , 21-24 Sept. 1999, pp:1323 – 1327.

[8] B. Dahill, B. Neil Levine, E. Royer and C. Shields, "A Secure Routing Protocol for Ad hoc Networks", Technical report UM-CS-2001-037, University of Massachusetts, Amherst, August, 2001.

[9] Y. Hu, A. Perrig, and D.B. Jonson, "Ariadne: A Secure On-Demand Routing for Ad hoc Networks", Proceedings of ACM MOBICOM 2002, pp:12-23, September 2002.

[10] Jameela Al-Jaroodi, "Security Issues In Wireless Mobile Ad hoc Networks (MANET)", Technical Report TR02-10-07, University of Nebraska-Lincoln, 2002.

[11] Y. Frankel, P. Gemmell, P. D. MacKenzie and M. Yung, "Proactive RSA", In Proceedings of CRYPTO 1997, Springer Verlag LNCS, pp: 440–454, 1997.

[12] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks", roceedings of ACM MOBIHOC 2001, pp. 299-302, October 2001.

[13] K. Sanzgiri, B. Dahill, B. Neil Levine, C. Shields and E. Royer, "A Secure Routing Protocol for Ad hoc Networks", Proceedings of IEEE ICNP 2002, pp: 78-87, November 2002.

[14] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002). S. 1-10. September 2002.

[15] Y.-C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks", Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, New York, USA, June 20-21, 2002.