International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:8, 2008

Secure Internet Connectivity for Dynamic Source Routing (DSR) based Mobile Ad hoc Networks

Ramanarayana Kandikattu, and Lillykutty Jacob

Abstract**—** 'Secure routing in Mobile Ad hoc networks' and 'Internet connectivity to Mobile Ad hoc networks' have been dealt separately in the past research. This paper proposes a light weight solution for secure routing in integrated Mobile Ad hoc Network (MANET)-Internet. The proposed framework ensures mutual authentication of Mobile Node (MN), Foreign Agent (FA) and Home Agent (HA) to avoid various attacks on global connectivity and employs light weight hop-by-hop authentication and end-to-end integrity to protect the network from most of the potential security attacks. The framework also uses dynamic security monitoring mechanism to monitor the misbehavior of internal nodes. Security and performance analysis show that our proposed framework achieves good security while keeping the overhead and latency minimal.

Keywords**—**Internet, Mobile Ad hoc Networks, Secure routing.

I. Introduction

MOBILE Ad hoc Network (MANET) has been a challenging research area for the last decade because of its versatility in routing, power constraints, security issues etc. A stand-alone MANET has limited applications because the connectivity is limited to itself. MANET user can have better utilization of network resources only when MANET is connected to the Internet. But, global connectivity adds new security threats to the existing active and passive attacks on MANET.

Many researchers proposed various solutions [1,2] to provide global connectivity to MANET. But, these proposals have not considered the security perspective of integrated network. Proposals [3,4,6,9] addressed the security threats and possible solutions for standalone ad hoc networks. These proposals have not considered the global connectivity of MANET and the related threats. Xie et al. [5] addressed the security framework for the integrated Internet-MANET. But their proposal depends heavily upon public key cryptographic algorithms, which are not desirable because of the computational overhead and latency problems. This paper proposes a framework that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security.

The rest of the paper is organized as follows. Section II explores the related work in the area of secure routing protocols for MANET. Section III presents a detailed description of the proposed framework. Section IV presents its security and performance analysis. Finally Section V is about conclusions and future work.

II. Related Work

In this section we explore some of the existing secure routing protocols for MANETs.

Xie and Kumar [5] and Jiang et al. [4] use digital signature based hop-by-hop authentication in the route discovery. As Route Request (RREQ) floods in the entire network, every node in the network gets involved in the signature generation and verification process, which consumes a lot of node's resources irrespective of whether the node is included in the route or not. Moreover, public key cryptography results in long processing delay and computational overhead.

Kargl et al. [9] proposed Secure Dynamic Source Routing (SDSR) for standalone networks. According to the proposal, each node along the route appends its *Diffie-Hellman public key* and encrypted hash of calculated session key, to the Route Reply (RREP) packet, while it traverses from the destination to the source. It increases the RREP packet size enormously. A RREP packet larger than the maximum payload of 802.11 MAC frame is to be forwarded to the next hop in multiple frames. It increases delay at each node and degrades the efficiency of routing protocol. In addition to that, the online computation of session key from the *Diffie-Hellman public key* also adds delay to the route setup process.

Pirzada et al. [10] use promiscuous mode to detect the attacks such as black hole, gray hole, modification fabrication attacks, etc. But techniques using promiscuous mode fail to work when an attacker uses unidirectional antennas and also fail to detect the collaborative attacks.

Manuscript received on October 9, 2007.

Ramanarayana Kandikattu is a Research Scholar in Department of Electronics and Communication Engineering, National Institute of Technology Calicut-673601, India (e-mail: k_ramnarayan@rediffmail.com).

Lillykutty Jacob, PhD, is Professor and Head of Electronics and Communication Engineering, National Institute of Technology, Calicut-673601, India.

III. Our Proposed Protocol: Secure Global Dynamic Source Routing Protocol (SGDSR)

A. Assumptions and Key Setup

We make similar assumptions as in [5,11] with SGDSR as well: i) Every Mobile Node (MN) in the MANET belongs to a certain administrative domain controlled by an agent called Home Agent (HA) and every MN shares a secret key with its HA; ii) Every node gets the digital certificate containing the [Node's Home Address, Public Key, Time of Issue, Time of Expiry] signed by a central Certificate Authority (CA) by some secure means, before entering into the ad hoc network, where CA's public key is known to HA, FA and all authorized MNs; iii) SGDSR requires pair-wise shared secret keys to be set up in each authorized node. It assumes that network has the mechanism to set up *pair-wise shared secret keys* in every node which are under one administrative domain. That means, every node in the network should share a secret key with every other node in the network, and hence each node should have (n-1) shared keys in a network of 'n' nodes.

Blundo et al. [12] introduces a promising solution for establishing pair-wise key setup in each node. It is a polynomial-based key pre-distribution protocol. In this proposal, the key distribution centre generates the polynomial share of node 'a', $f(ID_a,y)$, from a randomly generated bivariate k-degree polynomial, $f(x,y)$, by substituting $x=ID_a$. Node 'a' can compute the shared key $f(ID_a, ID_b)$with node 'b' by substituting $y=ID_b$, in its polynomial share. In this method, a node need not store all the (n-1) shared keys. It can compute the shared keys on demand with the help of its polynomial share. The memory requirement for storing polynomial is minimal.

B. Design Goals

The following are the design goals of SGDSR:

- To provide security against modification, fabrication, replay, and impersonation attacks on Intra-MANET routing as well as Internet-MANET routing.
- Low security overhead.
- Low route setup delay and communication overhead.

C. Protocol Description

SGDSR is designed to protect two communication scenarios: i) Internet-MANET communication; and ii) Intra-MANET communication.

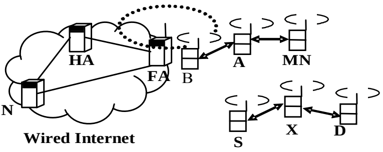


Fig. 1 Internet connectivity to MANET using Mobile IP

In Fig. 1 the communication between MN and CN is Internet- MANET communication with the help of multi-hop connectivity through intermediate nodes A, B and FA. The communication between S and D through the intermediate node X is Intra-MANET communication.

1) Internet-MANET Communication

As soon as a node enters the network, it determines whether it is in its home network or foreign network by comparing the network prefix of its home address with the network address learned from agent advertisements. If they are same it comes to the conclusion that it is in the home domain else it is in the foreign network.

When a node is in the home network it can get Internet connectivity through HA. It can also take part in the Intra-MANET communication with its home address and *digital certificate* and its *polynomial share*.

When the node is in the foreign network it has to register its *Care-of-Address* (CoA) with HA using Mobile IP protocol and should also obtain temporary certificate certifying its CoA and public key from CA through FA. It also needs to obtain its *polynomial share* from the FA; otherwise node is not allowed to participate in ad hoc routing. Table I shows the notations used in the proposed framework.

TABLE I
Notations used in the Framework

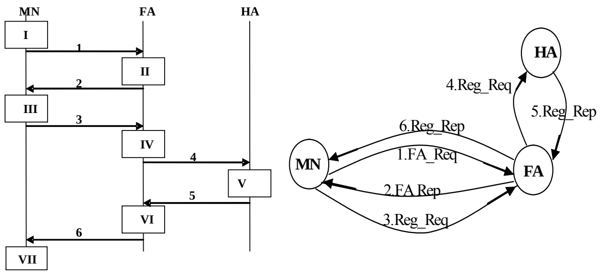
MN→A	Message transmission from MN to A
x,y	concatenation of two messages x and y
MN_{CoA}	MN's Care of Address
$FA_{Multicast}$	Foreign Agent's Multicast Address
FA	Foreign Agent's IP Address
ID	Route Message Unique ID
Dx	Diffie-Hellman publuc key of node x
{ }	Route Record
h_1	Hash code on (Randon nonce,Route Record)
h_n	Hash code on (h_{n-1},Route Record)
Sig_x	Signature of Node x on static part of message
$Cert_x$	Certificate of node x
FA_Req	A bit sequence indicating FA Request
FA_Rep	A bit sequence indicating FA Reply
R_Req	A bit sequence indicating Route Request
R_Rep	A bit sequence indicating Route Reply
R_Err	A bit sequence indicating Route Error
R_Report	A bit sequence indicating Route Report
K_{x-y}	Shared secret key between node x and node y
H_{x-y}	Hash code on the K_{x-y} and the specified message
H(m)	Hash on message m

2) FA Discovery and Registration Process

The salient steps involved in the secure registration of CoA with HA are depicted in Fig. 2a, where I to VII show the processes at the concerned node and 1 to 6 correspond to the control message flow between different nodes. Fig. 2b depicts the control messages that flow between MN, FA and HA.

Process I: MN which enters the foreign network initiates FA discovery process by generating FA_Req message (Step 1.1 in Fig. 3) with its home address as the source address and agent's multicast address 224.0.0.11 as the destination address. MN appends a hash tag h_1=hash (a random nonce, {MN}) to protect the source route from alteration. MN signs on the static message with MN's private key, i.e., Sig_{MN}=

K^{-1}_{MN}[Hash (FA_Req , $MN_{HA,}$ $FA_{multicast,}$ ID, D_{MN})] and broadcasts the message to its neighbors. FA_Req propagates to FA through nodes A and B.



a) Steps of registration process b) Control message flow

Fig. 2 FA discovery and registration process

Step 1.1 MN → A : FA_Req,MN_{HA},$FA_{Multicast}$,ID,D_{MN}, {MN_{HA}},h_1,Sig_{MN},$Cert_{MN}$

Step 1.2 A → B : FA_Req,MN_{HA},$FA_{Multicast}$,ID,D_{MN}, {$MN_{HA,}$A},h_2,Sig_{MN},$Cert_{MN}$

Step 1.3 B → FA : FA_Req,MN_{HA},$FA_{Multicast}$,ID,D_{MN}, {$MN_{HA,}$A,B},h_3,Sig_{MN},$Cert_{MN}$

Step 2.1 FA → B : FA_Rep,MN_{HA},$FA_{Multicast}$,ID, $D_{FA,}$ {$MN_{HA,}$A,B,FA},h_3,List of CoAs, $H_{FA-B,}$ Sig_{FA},$Cert_{FA}$

Step 2.2 B → A : FA_Rep,MN_{HA},$FA_{Multicast}$,ID, $D_{FA,}$ {$MN_{HA,}$A,B,FA},h_2, List of CoAs, $H_{B-A,}$ Sig_{FA},$Cert_{FA}$

Step 2.3 A → MN : FA_Rep,MN_{HA},$FA_{Multicast}$,ID, $D_{FA,}$ {$MN_{HA,}$A,B,FA},h_1, List of CoAs, Sig_{FA},$Cert_{FA}$

Fig. 3 Steps involved in FA Discovery

Step1.2: Any neighbor node A of MN receives FA_Req. It checks whether it has already seen the request. It drops any duplicate and invalid FA_Req; otherwise, it makes an entry in its *route request table* and then appends its IP address to the *route record* and replaces $h_1$with h_2=hash (h_1, {MN_{HA}, A}). Then node A broadcasts the message to its neighbors.

Step1.3: Any neighbor B of node A receives the message and then broadcasts the FA_Req to its neighbors after doing similar process.

Process II: Upon reception of FA_Req from node B, FA validates the signature. If the signature is valid, FA computes shared session key SK_{FA-MN} with the help of D_{MN} in the FA_Req packet. FA initiates FA_Rep (Step 2.1**)**. FA_Rep carries the actual IP address of FA and the list of CoAs. FA affixes H_{FA-B}= Hash (K_{FA-B}, SRM), where SRM=[MN_{HA},$FA_{Multicast}$,ID,D_{FA},{MN_{HA}, A,B, FA }, List of CoAs], and K_{FA-B} is the pair wise shared key between FA and B which is calculated using FA's *polynomial share.* FA unicasts FA_Rep back to node B.

Step 2.2: Upon reception of FA_Rep, node B first computes the hash code on the buffered h_2 and extracted part of source route from MN to itself from the *route record* available in the FA_Rep message and checks if it is equal to $h_{3.}$ The hash tag h_3 is to see that FA_Rep travels exactly in the reverse route and ensures that route is not modified. After passing the first check, node B computes the hash code of its shared key K_{FA-B} and SRM in the FA_Rep and checks if it is equal to H_{FA-B}. If so, node B authenticates FA. Then, it replaces H_{FA-B} in the FA_Rep packet with H_{B-A} and unicasts the FA_Rep to A.

Step 2.3: Finally Node A unicasts the FA_Rep to node MN if h_2 and H_{B-A} are valid.

Process III: Node MN checks h_1.Also validates the signature of FA. These verifications ensure that, the learned *source route* is not a fabricated or modified one. MN calculates shared session key SK_{MN-FA} using Diffie-Hellman public key $D_{FA.}$

Now both FA and MN are authenticated each other using digital certificates and can believe each other. MN chooses one CoA among the given list of CoAs and then initiates registration process with the message in Step 3 and unicasts the Reg_Req message to FA along the shortest among learned routes.

Step 3 MN → FA: Reg_Req,$M_{1,}H_{MN-FA}$
where M_1 =M, H_{MN-HA} and M= MN_{HA}, MN_{CoA} FA,ID, {MN_{CoA},A,B,FA},List of CoAs

H_{MN-HA} is the Hash(K_{MN-HA},M) used for checking integrity and authentication between MN and HA, and H_{MN-FA} is the Hash($SK_{MN-FA,}M_1$) used for checking integrity and authentication between MN and FA.

Process IV: Upon reception of Reg_Req, FA validates H_{MN-FA}. Then FA records MN's CoA, and signs message M_1 with its private key, appends its certificate and send the message to HA as in Step 4.

Step 4 FA → HA: $M_{2,}$ where M_2=[M_1,$D_{FA,}$ Sig_{FA},$Cert_{FA}$]

Process V: Upon reception of Reg_Req packet from FA, HA validates the signature of FA and H_{MN-HA}.This process ensures that: i) MN and FA authenticate each other; ii) FA has not modified the actual registration message sent by MN; and iii) message sent by FA is not altered.

After satisfying the verification results, HA calculates the session key SK_{FA-HA} with the help of Diffie-Hellman public key[14] D_{FA}..HA then registers MN's CoA and sends Reg_Rep (Step5) after signing the entire message with its private key.

Step 5 HA → FA: Reg_Rep,M, $D_{FA,}$ Sig_{HA},$Cert_{HA}$

Process VI: Upon reception of Reg_Rep, FA validates signature of HA, then computes session key SK_{HA-FA}. FA gets temporary certificate for MN from CA with the details: [CoA, public key, time of issue, Expiry time]. Then FA sends the Reg_Rep to MN after appending the encrypted MN's

Polynomial share as given in Step 6.

Step 6 FA → MN: Reg_Rep,M, Sig_{HA},$Cert_{HA,}$ Temp-$Cert_{MN,}$ $SK_{MN\text{-}FA}$ ($MN_{Polyshare}$),$H_{FA\text{-}MN}$

Process VII: MN validates $H_{FA\text{-}MN}$ and the signature of HA, then records its temp-certificate and decrypted polynomial share.

The registration process ensures pair wise mutual authentication among MN, FA and HA and there by avoids any fraudulent node to impersonate or manipulate registration messages.

Once the registration process is successfully completed, HA tunnels the packets destined for MN to FA. FA sends the packets to MN through multihop communication.

D. Intra-MANET Communication

Let node S wants to communicate with node D using SGDSR protocol. Let X be an intermediate node. SGDSR permits nodes to participate in the routing protocol only after acquiring the *certificate* and *polynomial share*. If a node is in its home network it can use its home address as its ID. If a node is in the foreign network, it has to complete the registration process first and then it can use the CoA as its ID.

Step 4.1 S → X: R_Req,S,D,ID,{S},h_1,$H_{S\text{-}D}$

Step 4.2 X → D: R_Req,S,D,ID,{S,X},h_2,$H_{S\text{-}D}$

Step 4.3 D → X: R_Rep,S,D,ID,{S,X,D},h_2,$H_{D\text{-}X}$

Step 4.4 X → S: R_Rep,S,D,ID,{S,X,D},h_1,$H_{X\text{-}S}$

Fig. 4 Steps involved in ad hoc route discovery

The source node S initiates route discovery process by generating R_Req. The sequence of steps involved is given in Fig. 4.

Source S generates R_Req with its IP address as source ID, destination address as destination ID. It appends h_1=Hash (nonce,{S}), and $H_{S\text{-}D}$ =Hash ($K_{S\text{-}D,}$ [S,D,ID]) and broadcasts to its neighbors.

A neighbor X to node S receives the R_Req and then appends its ID to the *route record* and replaces h1with h_2=hash (h_1, {S, X}) and then broadcasts the R_Req to its neighbors.

Upon reception of R_Req, node D first validates $H_{S\text{-}D}$ to check the integrity of packet and to authenticate the sender. Upon validation, node D generates R_Rep as in step 4.3. D appends the hash code $H_{D\text{-}X}$ =Hash ($K_{D\text{-}X,}$ [S,D,ID,{S,X,D}]) to R_Rep and then unicasts the message to node X, which in turn unicasts the R_Rep, to node S, after validating h_2 and $H_{D\text{-}X}$.

Finally, Node S records the source route in its route cache, after validation of h_1 and $H_{X\text{-}S}$. Now the node S sends the data packets using the source route.

Route Maintenance: Every node in the route keeps track of the link between itself and next hop neighbor. If the link is found broken, node generates R_Err and signs with its private key, then unicasts to the source node thorough the intermediate nodes. Upon validation of signature, source node may select an alternative route stored in its route cache. If no route is available source initiates route discovery again.

E. Reactive Security Mechanism

SGDSR is supported by a reactive security mechanism similar to Watch Dog [13], to mitigate the threats due to intermediate nodes. The security mechanism works as follows.

The sender node buffers the packet, transmits the packet to the next hop node and then switches itself into the promiscuous mode to over hear the retransmission by recipient node. Sender compares the buffered packet and overheard packet. From this observation sender node can find out whether the recipient node is carrying out any attacks such as black hole, modification, fabrication, impersonation, and replay attack.

If a next hop node is found guilty, the sender node informs about the misbehavior to the source node in a special packet R_Report after attaching its signature. Source node forwards the R_Report to the FA after signing the message. It is the responsibility of FA to inform about the misbehavior to the malicious node's HA in order to eliminate it from the network.

F. Optimizations

The proposed SGDSR protocol is the security extension of Dynamic Source Routing (DSR) protocol[7]. It does not allow all the optimizations possible for DSR; rather, the following optimizations are allowed:

- An intermediate node, which knows the valid route to the destination, unicasts the route request packet in the shortest known route to avoid unnecessary flooding.
- All the authorized nodes of SGDSR have a common network prefix in their IP address. Hence, host part of IP address can be used as node's ID to reduce the size of route record in the control and data packets. In this case, the *network part of address* and *subnet mask* fields should be included in the packet header in order to reconstruct any node's IP address unambiguously.

IV. Security and Performance Analysis

A. Security Analysis: Intra-MANET Communication

The proposed SGDSR protocol is secure against most of the external attacks, because of the following three phases of defense:

- A mobile node is permitted to participate in the routing protocol only after successful registration with its HA. This process helps:
- To filter out external malicious nodes from entering the network.
- To bind a unique IP address with the ad hoc ID of the node. IP address is not only useful to uniquely

identify the node in the global communication scenario but also helps to fix accountability to the participating nodes. Any registered node found guilty can be fixed and such nodes can be eliminated from the network. This enhances trust levels among the members of the network.

- The static part of route request messages is protected by a hash code function to detect tampering of static part by intermediate nodes. The mutable part is protected by another hash code function to restrict the route reply traversal exactly in the reverse order of learned route. This process avoids modification and fabrication attacks on the source route. End-to-end authentication in the route request phase avoids impersonation of source and destination nodes. End-to-end integrity in the route request phase avoids modification attacks by intermediate nodes. Hop-by-hop authentication in the route reply phase avoids external malicious nodes to participate in the routing protocol and thereby avoids the attacks caused by them.
- Reactive security mechanism added into the protocol finds out the malicious operations and consequent attacks caused by the internal authenticated nodes, which can not be detected by proactive security methods. Black hole and gray hole attacks are some such attacks.

B. *Security Analysis: Internet Connectivity*

The security perspective of registration process is discussed here.

The mutual authentication of MN, FA and HA is carried out with the help of public key and shared key cryptography techniques.

The secure registration process adopted in the protocol gives no scope for impersonation, modification, and fabrication attacks by any fraudulent node.

C. *Performance Analysis: Computational Overhead*

The computational overhead of SGDSR is very low compared to the existing protocols [5, 9] due to the following factors:

SGDSR uses minimal public key cryptography in the FA discovery and registration process. Table 2 gives a comparison with [5]. SGDSR requires no sign generation/verification at intermediate nodes. SGDSR uses keyed hash function for hop-by-hop integrity and authentication, which is computationally economical, where as [5] requires four public key signature generation and verifications at each intermediate node between MN and FA to complete the registration process.

A very important difference between [5] and SGDSR is that, proposal [5] uses public key based sign generation and verification for hop-by-hop authentication in the route request phase, which floods the entire network. Every node has to do at least one sign generation and one sign verification irrespective of whether it belongs to the route or not. SGDSR uses light weight hash codes for this purpose, which greatly reduces the computational load as well as processing delay at each node, with out compromising security

TABLE II
COMPUTATIONAL LOAD FOR REGISTRATION PROCESS

	Xie [5]				SGDSR			
	At MN	Int. Node	At FA	At HA	At MN	Int Node	At FA	At HA
No of Cert verifications	0	0	1	1	2	0	2	1
No. of Public key Sign gen.	1	4	3	1	1	0	2	1
No. of Public Key Sign Ver.	2	4	3	1	2	0	2	1

SDSR [9] appends Diffie-Hellman public key to the route reply, for hop-by-hop authentication as well as for distribution of shared session keys among the members of the route, which increases the size of route reply packet enormously as the number of hops increases. Its adverse effects are: i) increase in communication overhead, and ii) enormous increase in processing delay due to online computation of session key and its hash value. SGDSR uses pair wise shared key pre_distribution for this purpose.

V. CONCLUSIONS AND FUTURE WORK

Though there are many research proposals on 'Internet connectivity for ad hoc networks' and 'Secure routing protocols for ad hoc networks', separately, the research on the 'secure routing protocols for integrated Internet-MANET' is lacking. In this paper we proposed a secure routing protocol for global connectivity of DSR based MANET. Proposed protocol SGDSR uses hash codes extensively to minimize the computational and communication overhead. SGDSR is resistant to most common security attacks such as modification, fabrication, replay attacks and it can also detect black hole, gray hole attacks etc., with the help of reactive security mechanism.

Routing delay is another important consideration. Public key based computation intensive secure routing protocols can not work well due to the longer processing delay, especially in ad hoc networking environment. SGDSR is a carefully designed light weight protocol for secure global connectivity, and with minimal overhead and latency.

Future work includes security analysis of the proposed protocol using BAN logic and performance analysis of the protocol using OPNET simulation software. We are also working towards the design of an efficient reactive security mechanism, and the design of efficient key setup using Identity-based cryptosystem to support the protocol.

REFERENCES

[1] Y. Sun, E.M. Belding-Royer, and C.E. Perkins: "Internet Connectivity for Ad hoc Mobile Networks," International Journal of Wireless

Information Networks special issue on Mobile Ad Hoc Networks (MANETs): Standards, Research, Applications, 9(2), April 2002.

[2] P. Ratanchandani and R. Kravets: "A hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks", Proceedings of IEEE WCNC, 2003.

[3] Panagiotis Papadimitratos and Zygmunt J. Haas: "Secure Routing for Mobile Ad Hoc Networks" In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).

[4] Tingyao Jiang, Qinghua Li, Youlin Ruan: "Secure Dynamic Source Routing Protocol" Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'04) - Volume 00, (2004), Pages: 528 – 533.

[5] Bin Xie, and Anup Kumar: "A Framework for Internet and Ad hoc Network Security", IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

[6] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer: "A secure routing protocol for ad hoc networks", Proceedings of the 10th IEEE International Conference on Network protocols (ICNP'02).

[7] D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. G. Jetcheva: "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", http:// www.ietf.org /internet-drafts /draftietf -manet-drIETF draft, 2004.

[8] C. Perkins: "IP Mobility Support for IPv4," IETF RFC 3220, 2002.

[9] F. Kargl, A. Geiß, S. Schlott, M. Weber: "Secure Dynamic Source Routing", Hawaiian International Conference on System Sciences 38, Hawaii, USA, January 2005.

[10] Asad Amir Pirzada Chris McDonald, Amitava Datta: "Performance Comparison of Trust-Based Reactive Routing Protocols" IEEE Transactions on Mobile Computing, Vol. 5, Issue 6, (June 2006) Pages: 695 – 710.

[11] Leiyuan Li , Chigan C: "Token Routing: A Power Efficient Method for Securing AODV Routing Protocol", Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Control, 2006. ICNSC '06, (April 2006) pages 29- 34.

[12] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung: "Perfectly-secure key distribution for dynamic conferences", In Advances in Cryptology – CRYPTO '92, LNCS 740, (1993)pages 471–486.

[13] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker: "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks". In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000.)

[14] Whitfield Diffie and Martin Hellman: "New directions in cryptography", IEEE Transactions on information Theory, V olIT-22, no6, (Nov, 1976) pp. 644-654.