FOUNDATIONS OF COMPUTING AND DECISION SCIENCES
Vol. 39 (2014) No. 2

DOI: 10.2478/fcds-2014-0008 ISSN 0867-6356
e-ISSN 2300-3405

RSRP: A Robust Secure Routing Protocol in MANET

Ditipriya SINHA[1], Uma BHATTACHARYA[2], Rituparna CHAKI[3]

Abstract. In this paper, we propose a novel algorithm **RSRP** to build a robust secure routing protocol in mobile ad-hoc networks (MANETs). This algorithm is based on some basic schemes such as RSA_CRT for encryption and decryption of messages; CRT for safety key generation, Shamir's secret sharing principle for generation of secure routes. Those routes which are free from any malicious node and which belong to the set of disjoint routes between a source-destination pair are considered as probable routes. Shamir's secret sharing principle is applied on those probable routes to obtain secure routes. Finally, most trustworthy and stable route is selected among those secure routes. Selection of the final route depends on some criteria of the nodes present in a route e.g.: battery power, mobility and trust value. In addition, complexity of key generation is reduced to a large extent by using RSA-CRT instead of RSA. In turn, the routing becomes less expensive and most secure and robust one. Performance of this routing protocol is then compared with non-secure routing protocols (AODV and DSR), secure routing scheme using secret sharing, security routing protocol using ZRP and SEAD depending on basic characteristics of these protocols. All such comparisons show that RSRP shows better performance in terms of computational cost, end-to-end delay and packet dropping in presence of malicious nodes in the MANET, keeping the overhead in terms of control packets same as other secure routing protocols.

Keywords: CRT, Shamirs' secret sharing, safetykey, trust agent, suspect node

[1] Assistant Professor, Department of Information Technology, CIEM, Kolkata 700040, India. email: ditipriya_sinha@yahoo.co.in Phone: +919836732484

[2] Professor, Department of Computer Science & Technology, Bengal Engineering & Science University, Shibpur, Howrah 711103, India. email: ub@cs.becs.ac.in Phone: +919830899022

[3] Associate Professor, Department of Computer Science & Engineering,West Bengal University of Technology, Kolkata 700064, India. e
mail: rchaki@ieee.org Phone: +919830507213

1. Introduction

Application of mobile ad-hoc networks are extended to military service, emergency service, confidential video conferencing etc. which makes security issue to play an inevitable role in this field. Every node in MANET is identical with respect to all functionalities.

Key generation, encryption and decryption play an important role for providing secure routing in MANETs. However these schemes increase computational overheads for all nodes in the network. The RSA algorithm involves three steps: key generation, encryption and decryption. RSA [16] involves a public key and a private key**.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. Chinese remainder theorem (CRT) uses the result about congruence in number theory and its generalizations in abstract algebra.. In RSA-CRT, it is a common practice to employ the Chinese Remainder Theorem during decryption which results in a decryption much faster than modular exponentiation used in RSA.

Secret sharing in MANETs is a challenging issue due to its dynamic nature. Many researchers are involved in solving the secret sharing problem. Shamir's [20] proposal is one of the eminent secret sharing schemes. This scheme uses the concept of Lagrange's Interpolation method, a popular technique for polynomial evaluation. Shamir's scheme divides the data packet into n pieces such that it can be easily reconstructed from any $k = \left\lfloor \frac{n}{2} \right\rfloor$ number of pieces.

Main objective for secure routing is that data should be transmitted in secure and confidential way from source to destination. Trust value, battery power and stability of the nodes are the factors or attributes for determining a reliable, stable and trustworthy path in between a source-destination pair. Absence of any attributes of them may make the path unreliable.

A new security scheme has been proposed in this paper for MANETs. This paper uses RSA- CRT scheme for its high efficiency in key generation, encryption and decryption of data. For secure route detection a safety key is generated. This safety key is divided into n pieces and propagated through n different available routes in between a source-destination pair. Safety key can easily be reconstructed from any $k = \left\lfloor \frac{n}{2} \right\rfloor$ pieces. Secure paths are detected with the help of Shamir's secret sharing using Lagrange's Interpolation scheme. Final route amongst those is chosen by using the criteria of a stable and trustworthy path i.e. trust value, battery power and stability of the nodes.

Section 2 contains review of past works related to the area, Section 3 contains scope of the work, proposed secure routing protocol is described in section 4, performance of the proposed protocol has been evaluated in section 5 and conclusion has been drawn in section 6.

2. Review of Past Works

This section reviews several security solutions in mobile ad hoc network. Especially this section investigates different key generation model for encryption and decryption, secret

sharing and its application model, authentication based secure routing model and other secure routing model since these models demonstrate the gradual progress in the literature.

2.1. Key generation for encryption and decryption

RSA [16] technique is the example of asymmetric key cryptography. Rivest, Shamir and Adoreman established this technique. This technique uses two keys, public and private. Source node encrypts message using its public key and destination node decrypts that ciphertext message using its private key. Chinese Remainder Theorem [21] is simple mathematical result. This theorem helps design of deterministic key pre-distribution using number theory. CRT generates key pool and key chain for key pre distribution. Fast Decryption Method for RSA Cryptosystem [6] designs new decryption method. It combines RSA with CRT and increases computational speed. This paper shows how CRT decryption gives better performance compared to RSA decryption method. RSA Cryptosystem Design Based on Chinese Remainder Theorem [24] proposes a systolic RSA cryptosystem based on a modified Montgomery's algorithm and the Chinese Remainder Theorem (CRT) technique. The CRT technique improves the throughput rate up to 4 times in the best case. This paper adds some control logic to accomplish some modular exponentiation operation. Provably-Secure Time-Bound Hierarchical Key Assignment Scheme [2] is a method to assign time-dependent encryption keys to a set of classes in a partially ordered hierarchy, in such a way that the key of a higher class can be used to derive the keys of all classes lower down in the hierarchy, according to temporal constraints. This paper designs and analyzes time-bound hierarchical key assignment schemes which are provably secure and efficient.

2.2. Secret sharing and its applications

Shamir's Secret Sharing [20] proposes a method for sharing secret. This paper shows how to divide data D into n pieces in such a way that D is easily constructed from any k pieces. This technique enables the construction of robust key management for cryptographic system. This scheme provides most secure key management scheme. Various secure routing protocols use this concept for key management

Secure Routing Scheme in MANETs using Secret Key Sharing [1] proposes a secret sharing scheme using Shamir's Secret Sharing method. Here secret is shared to detect malicious nodes in the network. For the key transmission RSA scheme is used in this paper. This scheme uses RSA modular expansion for decryption whose computational cost is higher than CRT method. Chinese Remainder Theorem-Based RSA Threshold cryptography based schemes for MANETs using Variable Secret Sharing Scheme [17] provides a promising secure network. This proposed scheme is based on Chinese Remainder Theorem under the consideration of Asumth-Bloom secret sharing. DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks [4] propose a new efficient distributed anonymous secure routing protocol (DASR).

Diffie-Hellman key exchange scheme is used in this scheme to share secret key KSR between the source and destination nodes. SPREAD: Improving network security by multipath routing in mobile ad hoc networks [12] presents a complementary mechanism to

enhance secure data delivery in a mobile ad hoc network. The basic idea is to transform a secret message into multiple shares, and then deliver the shares via multiple paths to the destination so that even if a certain number of message shares are compromised, the secret message as a whole is not compromised.

2.3. Authentication based secure routing protocol

Authenticated Routing for Ad-hoc Networks (ARAN) [5,26] proposes cryptographic certificates to prevent and detect most of the security attacks. This protocol introduces authentication, non-repudiation and message integrity as part of minimal security policy for the ad hoc environment. On Securing MANET Routing Protocol against Control Packet [18] secures routing protocols in MANETs from packet dropping. This paper focuses on dropping control packets. Dropping control packet may be beneficial for selfish nodes and malicious nodes. Here each node monitors its successor node. The node monitors forwarding of directed routing control packets.

2.4. Other secure routing protocols

Trust Based Secure Routing in AODV Routing Protocol [9, 13] proposes modified AODV routing protocol with node trust value. It required the following modification in the existing AODV [9] protocol; (i) Two new control packets TREQ (Trust Request), TREP (Trust Reply), (ii) Modified extended routing table with four new fields; positive events, negative events, route status, opinion. Using this approach, secure route can be established by calculating trust value of each node which is participating in the route establishment process from source to destination.

Secure Efficient Ad hoc Distance Vector (SEAD) [7] is a proactive routing protocol, based on the design of Destination Sequenced Distance Vector routing protocol (DSDV) SEAD provides a robust protocol against attackers trying to create incorrect routing state in other node by modifying the sequence number or the routing metric. But SEAD does not provide a way to prevent an attacker from tampering next hop or destination field in route update. I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks [11] is enhancement of SEAD. In this proposed protocol, called ISEAD, it can let the neighbors check the correctness of the hash value using its TELSA key and reduce the routing overhead. .Secure Destination-Sequenced Distance-Vector routing protocol (SDSDV) for ad hoc mobile wireless networks [15, 23] is based on the regular DSDV protocol. Within SDSDV, each node maintains two one-way hash chains about each node in the network. In comparison with the secure efficient distance vector (SEAD) protocol previously described in the literature provides only lower bound protection on the metrics, whereas SDSDV can provide complete protection. An Encryption Based Dynamic and Secure Routing Protocol for Mobile Ad-hoc Networks [19] proposes an efficient key management mechanisms for enforcing confidentiality, integrity and authentication of messages in ad-hoc networks. Secure Routing Protocol for Mobile Ad hoc Network [10] guarantees acquisition of correct topological information in timely manner. This protocol provides accurate connectivity information despite the presence of strong adversaries. Secure Data Transmission on Multiple Paths in Mobile Ad Hoc Networks [25] is based on multiple paths for mobile ad

hoc networks. The scheme focused its attention on privacy and robustness in communication. New Security Algorithm for Mobile Ad hoc Networks Using ZONAL ROUTING PROTOCOL (ZRP) [22] presents a secure communication between the mobile nodes. A scenario of data transmission between the two mobile nodes has been considered. Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node via the cluster head. The authentication service uses a key management to retrieve the public key, which is trusted by the third party for identification of the destination.

3. Scope of the Work

The proposed RSRP protocol deals with the problem of generation of a secure and stable route between a source-destination pair in MANETs. Following points need to be discussed in this context.

- Securing message transmission normally involves some encryption at source node and decryption at destination node of messages using RSA technique which leads to a large computational overhead.
- Also the presence of the malicious nodes in the network is the cause of packet loss during transmission of messages through those nodes. Identifying malicious nodes and avoiding them in the route of message passing may thus reduce the number of packet dropped and thus improved the performance in the network.
- Finding secure routes requires generating a Safety Key. Shamir's Secret Sharing scheme which may divide this Safety Key into n (number of available routes) pieces and this key can easily be reconstructed by using $k = \left\lfloor \frac{n}{2} \right\rfloor$ pieces out of them. Concept underlying this scheme may be used successfully to detect all secure routes.
- Three points to mention are that:
    1. All nodes in MANETs are subject to loss of battery power during message passing /encrypting/decrypting.
    2. Stability information about a node may be helpful to establish a stable route because a stable route must consists of a set of stable nodes.
    3. Trust value of a node will be higher if it takes part in processing of messages successfully from a source to the destination node.

In this context weight of a node may be considered as the summation of trust value , battery power and stability of the node. Amongst all secure routes detected by Shamir's Secret Sharing principle the route having highest average value of nodes may be selected as the final route for message transmission.

Thus motivation of our work is to:

1. use the less expensive scheme for encryption and decryption of messages.
2. find set of probable routes without having any malicious nodes to improve the network performance in terms of lesser number of packet drops in the network.
3. generate Safety Key and detect all secure routes using Shamir's Secret Sharing scheme.

4. detect finally the most stable and trustworthy paths among those secure paths for message transmission.

4. Proposed Secure Routing Protocol

Proposed secure routing protocol is discussed as follows:

4.1. Assumptions

i) Mobility model used here is random waypoint [3]. This model restricts movement of the mobile nodes to a rectangle. Each node picks a destination within the rectangle along with a speed. The node travels to the destination at that speed. Upon reaching the destination, the node selects and waits for a uniformly distributed pause time. After waiting, the node picks another destination and another speed, continuing the process. The parameters of this model are the minimum and maximum speed and the maximum pause time.
ii) No path loss exists.
iii) All nodes are GPS enabled.
iv) All nodes have their sequential identity number according to their entry.

4.2. Data Structure and Message Format

A. Data Structure

W_i: Weight of the node i.
Tv_i: Trust value of node i.
Bp_i: Battery Power of node i.
Bp_{iprev}: Battery power of node i before current processing takes place.
Mob_i: Mobility of node i.
$W - T_i$: Waiting time of node i.
a: Energy required for forwarding and receiving each message.
s_t: Total number of messages sent in during the time duration Δt.
r_t: Total number of messages received during the time duration Δt.
u: Number of encryption done by node i during the time duration Δt.
v: Number of decryption done by node i during the time duration Δt.
k: Energy required for each encryption.
l: Energy required for each decryption.
n: Number of available routes in the network in the time duration Δt.
hopcount: The number of nodes on a route with same sequence no in the time duration Δt.
$Avgr_{S,D}[j]$: Average weight of j^{th} route in between source destination pair S, D in the time duration Δt.

$forward\_count_i$: Number of messages sent by Trust Agent successfully via node i to a neighbor.
$tot\_forward\_message_{i:}$: Total number of messages sent by the Trust Agent via node i to a neighbor.
Tr: Identity of trust agent.
sus_{id}: Identity of suspicious nodes.
S : Identity of source node.
$Pk - i$: Public key of node i.
$Pv - i$: Private Key of node i.
D: Identity of destination node.
Routetable[ ]: Stores all probable routes between source and destination. Structure of the table: Sequenceno, Source node, List of nodes in the route, Destination node. This table is associated with each node.
$Malicious - id[\ ]$: Stores identities of all malicious nodes. This table is associated with each node
$Secure - route[\ ]$: Stores all secure routes between source and destination. Structure of this table: Sequenceno, Source node, List of nodes in the secure route, Destination node. This table is built within each node when the node becomes a source node.
$Suspectlist - TR[\ ]$: Trust Agent (TR) stores identities of suspicious nodes.
$Weight - table_i[\ ]$: This table contains weight information of node i. Structure of this table: Node id, Trust value, Battery Power, Mobility. This table is associated with each node.
$Destination - key - table_i[\ ]$: This table contains public key information of destination node. Structure of this table: destination node id, public key value of the destination node. This table is associated with source node i.
$Key - table_i[\ ]$: This table contains safety key, public key and private key information of node i. Structure of this table: Node-id, public key value, private key value, safety key value. This table is associated with each node.
I: Initiator node.
Threshold: Expected time to detect secure route between source destination pair already initialized.
$Time - observ_I^{TR}$: Observation time for initiator node I by trust agent TR.
t_{mon}: Monitoring time for initiator node I monitored by trust agent Tr.
$neighbor - list_i[\ ]$: List of neighbors of node i which contains neighbor node id k and trust value Tv_k .
$POINTTABLE_{SD}$: List of points obtained by S from D where each point (x_i, y_i) corresponds to each route.
$Time - out$: Expected time duration for receiving ACK message from next hop node after sending FINDNEIGHBOUR / RREQ messages.

B. Message Format

Table 1. Message Format

Message	Structure
$FIND - NEIGHBOUR\{initiator\}/\{New\}$	$\{initiator-id, Tv_{initiator-id}\}/\{NEW, Tv_{New}\}$
ACK	$\{next-hop-id, Tv_{nexthop-id}\}$
$TRUSTY\{initiator\}/\{New\}$	$\{initiator-id, neighbor-list_{initiator-id}, TR\}/\{NEW, neighbor-list_{NEW}, TR\}$
$TRUSTVALUE\{initiator\}/\{New\}$	$\{TR, initiator-id, Tv_{initiator-id}\}/\{TR, NEW, Tv_{NEW}\}$
$RREQ$	$\{sequenceno, S, list\ of\ next-hop-ids, hopcount, D, Pk-S\}$
$ACKN$	$\{sequenceno, S, list\ of\ next-hop-ids, hopcount, D, Pk-D\}$
$ALERT$	$\{TR, neighbor-list_{TR}, suspectlist[sus-id]\}$
$PointRequest$	$\{sequenceno, S, D, (x_i, y_i)\}$
$WEIGHT\_REQ$	$\{sequenceno, S, List\ of\ all\ node-ids\ in\ the\ route, D\}$
$ACKNW$	$\{sequenceno, node-id, Weight-table_i, S\}$

4.3. Definitions

Definition 1: Mobility of a node i having n number of neighbors is defined as the summation of difference of distance computed between the node and all its neighbors during time interval Δt, i.e.,

$$\text{mob}_i = \sum_{s=1}^{n} \text{dist}(i, s) \quad (1)$$

where, $dist(i,s) = |d^t{}_{si} - d^{t+\Delta t}{}_{si}|$, where s being a neighbor of node i, $d^t{}_{si}$ indicates distance between node s and node i at time t. The distance is calculated from the location co-ordinates of the nodes at that instant of time.

Stability of the node is defined as the inverse of its mobility.

Definition 2: Battery power consumption of i^{th} node (Bp_i) is proportional to energy required for forwarding and receiving number of packets by the node during a specific time interval Δt and also number of encryption and decryption done by node i during the same time interval.

BP_i is defined as follows:

At the source and destination node,

$$BP_i = BP_{iprev} - \sum_{t=T}^{T+\Delta t} a * (s_t + r_t) + (u * k + v * l) \quad (2)$$

At any intermediate node,

$$BP_i = BP_{iprev} - \sum_{t=T}^{T+\Delta t} a * (s_t + r_t) \quad (3)$$

Battery power is computed when any processing such as forwarding/receiving or encrypting/decrypting packets takes place.

Definition 3: Trust value Tv_i of a node i is defined as follows:

$$Tv_i = {}^{forward\_count_i}/_{tot\_forward\_message_i} \quad (4)$$

Definition 4: Weight of a node i (W_i) is defined as the summation of its trust value, battery power and stability of the node at that time.

$$W_i = Tv_i + Bp_i + {}^{1}/_{Mob_i} \quad (5)$$

4.4. Some basic schemes used in secure routing

The proposed logic uses two keys for message encryption and decryption, RSA technique for encryption of data, CRT technique for decrypting data, safety key to detect the routes without having any malicious node between a source destination pair and Shamir's secret sharing principle to detect secure routes.

A. Key Generation

1) Each node i generates two prime numbers p and q so that $N = pq$ and $\acute{\emptyset}(N) = (p-1)(q-1)$.
2) Choose e such that e is not divisor of $\acute{\emptyset}(N)$ and $1 < e < \acute{\emptyset}(N)$.
3) d is the modular multiplicative inverse of $e (\mathrm{mod}\ \acute{\emptyset}(N))$.
   $e.d = 1 \bmod \acute{\emptyset}(N)$
4) (e, N) is the public key and (d, N) is the private key of node i.

B. Encryption using RSA at source node

When source node wants to encrypt message M to Ciphertext C for sending it to destination node, it uses public key of destination node using RSA in the way as described below:

$$C = M^e \ (\mathrm{mod}\ N) \quad (6)$$

C. Decryption using CRT at destination node

When destination node receives the encrypted message it decrypts this encrypted message using CRT following way:

$$\begin{aligned} dp &= d \bmod (p-1) \\ dq &= d \bmod (q-1) \\ q_{inv} &= q^{-1} \bmod p \\ m_1 &= c^{dp} \bmod p \\ m_2 &= c^{dq} \bmod q \\ h &= (q_{inv}(m_1 - m_2)) \bmod p \\ M &= m_2 + h * q \end{aligned} \tag{7}$$

D. Safety Key Generation using CRT

Safety key (SF) is a key which is used to detect secure routes among all available routes. Source node generates n integers $m_1, m_2, m_3, \ldots\ldots m_n$, such that gcd ($m_i$, m_j)=1. Then this key is generated by using following equations:

$z_i = {}^{m}/_{m_i}$, $y_i \equiv z_i^{-1} (\bmod m_i)$ and $Z \equiv a_1 (\bmod m_i) \equiv a_2 (\bmod m_2) \ldots \equiv a_n (\bmod m_n)$

Here (mod m_i) stands for moduler multiplicative inverse operation.

$$SF = a_1 y_1 z_1 + \ldots + a_n y_n z_n \tag{8}$$

Before sending message source node S generates Safetykey SF_s using CRT.

E. Secure Route Detection Scheme using Shamir's secret sharing.

As by the proposed solution source node S divides Safety key SF_s into n parts, where n is the number of available routes from source to destination. Now source node generates a polynomial F(x) of degree floor(n/2)-1=k-1 such that,

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{9}$$

where $a_0, a_1, \ldots a_{k-1}$ are set of integers.

Source node generates n number of points from this polynomial which are $((x_0, y_0); (x_1, y_1); \ldots\ldots; (x_{n-1}, y_{n-1}))$ and sends each of these points in encrypted form [section 4.4 B] through each amongst n different available routes to destination node. Destination node decrypts [section 4.4 C] those n points and again encrypts [section 4.4 B] those points and sends to the source node by backtracking in the same route.

Now source node decrypts those n points and takes any k points among them to regenerate the polynomial $F_1(x)$ using Lagrange's Interpolation such that,

$$F_1(x) = \sum_{r=0}^{k-1} y_r \prod_{i=0, i\neq r}^{k-1} \frac{(x - x_i)}{(x_r - x_i)} \tag{10}$$

The first constant part of $F_1(x)$ is called SF_1. If $SF_S = SF_1$, those *k* points are valid points and the routes used by those k points are also valid and hence secured. Otherwise at least

one of the routes used by those k points are not secured. ${}^{n}C_{k}$ number of combinations are available for computing Safety key. Those combinations generating correct value of Safety key will correspond to the respective secure routes.

4.5. Modules used in RSRP

The proposed routing is a 4-phase one: (i) Assignment of Trust values to all nodes in MANET (ii) Detection of Malicious node (iii) Detection of Probable Routes (iv) Detection of Secure Routes (v) Detection of Final Route.

4.5.1. Assignment of Trust Values to All Nodes in MANET

A. Initialization of Trust values at the beginning (Initialize-trust-manet())

Assumption: There are a few nodes closely placed in the MANET so that each node i is at a distance of one hop to each other and trust values (Tv_i) associated with each of them is initially zero. Time-out value is initialized to the expected value as defined in section 4.2A.

1. Arbitrarily, a node is chosen as Initiator node (I). , $W - T_I = 0$ //Initialization//
   It broadcasts its identity to its neighbors using $FIND - NEIGHBOUR\{\text{initiator} - \text{id}\}$ message [Section 4.2B].

2. while ($W - T_I < \text{time} - \text{out}$)
   do
   {
   I accepts ACK messages [section 4.2.B] from neighbor nodes within one hop distance and adds in its $\text{neighbor} - \text{list}_I$ [section 4.2.A].
   $W - T_I = W - T_I + 1$
   }

   I selects any one node of them as Trust Agent (TR) randomly and sends $TRUSTY\ \{initiator\}$ message [section 4.2.B] to all next-hop nodes including TR.

3. Count=0;
   Label: $C=0$; $\text{Time} - \text{observ}_I^{TR} = 0$ //Initialization//
   Monitoring Time $Time - observ_I^{TR}$ for the initiator node by Trust agent TR is

initialized as t_{mon} .

//Initialization//

while ($\text{Time} - \text{observ}_I^{TR} < t_{mon}$) //Computation of Trust value of node I by TR starts//

do

{

TR sends number of messages to another node j present in the $\text{neighbor} - \text{list}_{TR}$ using node I as the intermediate node.

$\text{Time} - \text{observ}_I^{TR} = \text{Time} - \text{observ}_I^{TR} + 1$

}

TR counts number of messages sent (m), messages successfully delivered (c) by using number of acknowledgement messages obtained from j. TR computes the trust value Tv_I of the initiator node [Section 4.3, Definition 3] and sends $TRUSTVALUE\{initiator\}$ message [section 4.2B] to the node I.

$count = count + 1;$

if ($c <= .3 * m$)

then

TR adds node I to $Suspect - list\ [Sus - id]$.

. else

if $count < 2$

then

$Temporary = TR; TR = I; I = Temporary.$

go to $Label$. // It reverses the role of Initiator node and Trust Agent node and in this way when $count = 1$, the trust value of the new Initiator node has been computed already .//

else // $count >= 2$, Trust value of the initiator node and the trust agent have been computed already in this situation.//

if there exists any remaining node in the $neighbor - list_I$

then Initiator node = next available node in $\text{neighbor} - \text{list}_I$

go to $Label$.

else stop. // computation of trust value of all nodes in the $neighbor - list_I$ is completed.//

B. Computation of Trust value for the newly entrant node (New-entry-trust())

1. On entry, a new node NEW broadcasts its identity to its neighbors using $FIND - NEIGHBOUR\{NEW\}$ message [section 4.2.B].

Initially $Tv_{new} = 0$ and $W - T_{NEW} = 0$

2. while $(W - T_{NEW} < Time - out)$

do

{

The nodes within one hop distance send an ACK message to NEW and NEW adds id of that nexthop node (k) with its trust value Tv_k to its $neighbor - list_{NEW}$.

$$W - T_{NEW} = W - T_{NEW} + 1$$

}

3. Node NEW selects the node i as Trust Agent (TR) having maximum trust value from its $neighbor - list_{NEW}$ and sends its $neighbor - list_{NEW}$ to TR through $TRUSTY\ \{NEW\}$ message [section 4.2.B].

4. $Time - observ_{NEW}^{TR} = 0$ //Initialization//

while **(** $Time - observ_{NEW}^{TR} < t_{mon}$)

do

{

TR sends number of messages to another node j present in the $neighbor - list_{TR}$ using node NEW as the intermediate node.

$$Time - observ_{NEW}^{TR} = Time - observ_{NEW}^{TR} + 1$$

}

TR counts number of messages sent (m), messages successfully delivered (c) by using number of acknowledgement messages obtained from j. TR computes the trust value Tv_{NEW} [Section 4.3, Definition 3] of the newly entrant node and sends it to the node NEW through the message $TRUSTVALUE\ \{NEW\}$ [Section 4.2.B].

if (c <= .3 * m)

then

TR adds NEW to Suspect − list [Sus − id] .

else

TR sends Tv_{NEW} to NEW through $TRUSTVALUE\{NEW\}$ message [Section 4.2.B].

5. Stop**.**

4.5.2. Detection of Malicious node(Maliciousdetect())

1. For each node belonging to $Suspectlist\ [Sus - id]$

do

{

$W - T_{TR} = 0$ //Initialization//

while ($W - T_{TR}$ < threshold)

do

{

TR observes all the values in $Tv_{\text{suspectlist[Sus−id]}}$

$W - T_{TR} = W - T_{TR} + 1$

}

if value of $Tv_{\text{suspectlist[Sus−id]}}$ remain same for the duration starting from detection of Probable Routes [section 4.5.3] to Detection of the Final Route [section 4.5.5]

then

TR declares the node $Suspectlist[Sus - id]$ as malicious one and sends $ALERT$ message [section 4.2.B] to all its neighbors present in its $neighbor - list_{TR}$ so that they update their list of malicious nodes.

}

4.5.3. Detection of Probable Routes (Probableroute( ))

Initially $i = 1,\ next - hop - id - 1 = 0,\ hopcount = 1,\quad W - T_S = 0,$ $Temp = S$

1. while ($W - T_S < Time - out$)

{

L : Temp broadcasts $RREQ\{sequenceno, Temp, next - hop - id - 1, \dots, next - hop - id - i, hopcount, D, Pk - S\}$ messages to all nodes within one hop distance.

if $next - hop - id - i \neq D$

then

$next - hop - id - i$ adds its id to $RREQ$ packets.

$hopcount++,\ W - T_S{+}{+},\quad i++,\quad Temp = next - hop - id - i,$

$next - hop - id - i = 0.$

go to L.

else

$next - hop - id - i$ copies $hopcount$ list from each $RREQ$ packet in each $ACKN$ message with same $sequenceno$ and sends $ACKN$ to S backtracking the same route traversed already.

break.

}

2. S accepts all $ACKN$ messages for the duration $Time - out$. Source S now checks if any node mentioned in $ACKN$ message is present in Malicious-list by calling *malicious-detect( ) module.* [Section 4.5.2]

if present,

then respective $ACKN$ message will be discarded

else

S stores the route obtained from the $ACKN$ messages in its $Routetable$ and also stores public key of D in its $Destination - key - table_S$ [Section 4.2.A].

3. Stop.

4.5.3. Detection of Secure Routes (Secureroute( ))

1. Source S generates safety key SF_S [Section 4.4.D] and stores it in its $Key - table_s$ [Section 4.2.A, 4.4.A]

2. Source S counts number of available routes from its $ROUTETABLE$ [ ] [Section 4.2.A].

count = n ./* n stands for number of available unique routes */

3. S generates a polynomial F(x) of degree

$$k\text{-}1 = \left\lfloor \frac{n}{2} \right\rfloor \text{-}1$$

such that,

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

S generates *n* number of points from F(x), such as $((x_0, y_0); (x_1, y_1); \ldots\ldots; (x_{n-1}, y_{n-1}))$

4. S calls RSA $\big((x_0, y_0); (x_1, y_1); \ldots\ldots; (x_{n-1}, y_{n-1})\big)$to encrypt those n points using [Section 4.4.B]. For encryption S uses public key of destination node D ($Pk - D$) from $Destination - key - table_S$.

5. For all routes present in *ROUTETABLE* (S, D) S sends each encrypted value of (x_i, y_i) through each route by using the message $PointRequest$ [Section 4.2.B].

6. For each (x_i, y_i) D calls CRT (x_i, y_i) to decrypt each (x_i, y_i) using [Section 4.4.C].

7. Again D calls RSA (x_i, y_i) to encrypt [Section 4.4.B] those n points and sends to S backtracking in the same unique routes traversed by using the message $PointRequest$ [Section 4.2.B].

8. $W - Ts = 0$ // Initialization //

while ($W - Ts <= time - out$)

do

{

S stores each (x_i, y_i) in its $POINTTABLE_{SD}$ [Section 4.2.A].

$W - Ts = W - Ts + 1$

}

9. S creates ${}^{n}C_{k}$ combination of sets where each set contains k out of n number of points.

10. For each set of k points S regenerates the polynomial $F_1(x)$ using Lagrange's Interpolation such that,

$$F_1(x) = \sum_{r=0}^{k-1} y_r \prod_{i=0, i\neq r}^{k-1} \frac{(x - x_i)}{(x_r - x_i)}$$

11. if (Constant part of $F_1(x)$ = Constant part of $F(x) = SF_s$)

then

S stores the route information and *sequenceno* which corresponds to those k valid points to its $Secure - route$ $(sequenceno, S, List\ of\ next - hop\ nodes\ in\ the\ route, D)$ table.

goto step 10 until all ${}^{n}C_{k}$ combination of sets are examined.

12. Stop.

4.5.4. Detection of the Final Route (Finalroute())

1. S sends $WEIGHT\_REQ$ message to all nodes on each secure route obtained from its $SecureRoute$ table.

2. Each node in the $SecureRoute$ sends their weight table [] to S using $ACKNW$ message with same *sequenceno* as present in $WEIGHT\_REQ$ message.

3. S calculates weight of each node i (W_i) from its $Weight - table_i$ using [Section4.3,Definition 4]. S then calculates average weight ($AVGR_{S,D}[m]$) of all nodes

present in m^{th} route which possess the same *sequenceno*.

4. S selects route *j* as final route for which average weight $AVGR_{S,D}[j]$ is maximum.
5. S uses RSA to encrypt each message using public key $Pk - D$ of destination node D and sends all messages through this j^{th} route to destination node D.
6. After receiving each encrypted message D decrypts this message using its private key $Pv - D$ of *D* using CRT and sends acknowledgement message to S backtracking in the same route as traversed already. For each node i present in j^{th} route Trust value Tv_i and battery power consumption Bp_i will be incremented and re-computed [Section 4.3, Definition 3, Definition 2] respectively in the backtracking period.
7. Step 1 to step 6 are repeated after every Δt time interval.

4.6. Algorithm RSRP

Step 1: At the beginning Initialize-trust-manet( ) module in executed.

Step 2: For each source destination pair (S-D) S calls **Probableroute( )** module which returns all probable disjoint routes free from any malicious node between S and D.

Step 3: S calls **Secureroute( )** module which returns secure routes among all available routes.

Step 4: S calls **Finalroute( )** module which returns final route through which all packets are sent to D.

Step 5: If any new node i enters in the network **New-entry-trust( )** module is executed.

Step 6: After threshold interval *S* repeats step 2 to 5.

5. Performance Evaluation

Performance of the algorithm RSRP has been evaluated and outlined in the following subsections.

5.1. Performance metrics

Performance metrics used to evaluate our proposed protocol are packet dropped versus number of malicious nodes, computational cost versus number of nodes, end to end delay versus load in terms of number of messages and overhead in terms of control packets versus number of nodes.

5.2. Simulation environment

Performance of proposed protocol is analyzed using simulation techniques. Table 1 shows the simulation setting of the network environment. This protocol is simulated in NS2.29. Simulation environment of this protocol is Fedora 9. We use IEEE 802.11 for wireless LAN as MAC layer. The channel capacity of mobile node is 2 Mbps. In our simulation mobile nodes move in a 600*600 m^2 region for 125 second simulation time. Mobility model is considered here as random waypoint. It is assumed that each node moves independently with the same average speed 10 m/s and pause time is 0-25 second. No path loss is considered. The network size is varied as 10, 20, 30, 40 and 50 nodes. The simulated traffic is constant bit rate (CBR). Table 2 shows the simulation setting of the network environment.

Table 2. Simulation Environment

Name	Value
Channel	Wireless
Propagation	Two Way
Network Interface Type	Wireless Phy
Antenna	Omni Antenna
No of nodes	10 to 50
MAC	IEEE 802.11
Simulation Area	600*600 m^2
Timeout period	5.0 sec.

5.3. Results and Analysis

We have compared the performance of proposed protocols with other existing **non-secure** routing protocols such as *AODV* [14] and *DSR* [8] as well as secure routing protocols such as *Secure Routing Scheme Using Secret Sharing* [1], *New Security Routing Protocol Using ZRP* [22] and *SEAD* [7]. According to basic characteristics of above stated routing protocols, proposed protocol is compared with others.

A. Packet dropped vs. number of malicious nodes

This protocol RSRP is compared with two non-secure routing protocols *AODV* [14] and *DSR* [8] and also two secure routing protocols i.e.: *security algorithm using ZRP* [22]and *Secure Routing Scheme Using Secret Sharing* [1] which is described in Figure 1. Packet dropped in case of *RSRP* is much less compared to *AODV* and *DSR* when number of malicious node increases since both *AODV* and *DSR* are **non-secure** routing protocols. Comparison of *RSRP* with *secure routing scheme with secret sharing* and *new security algorithm using ZRP* shows that its performance is best amongst three because of the novelty of the algorithm RSRP.

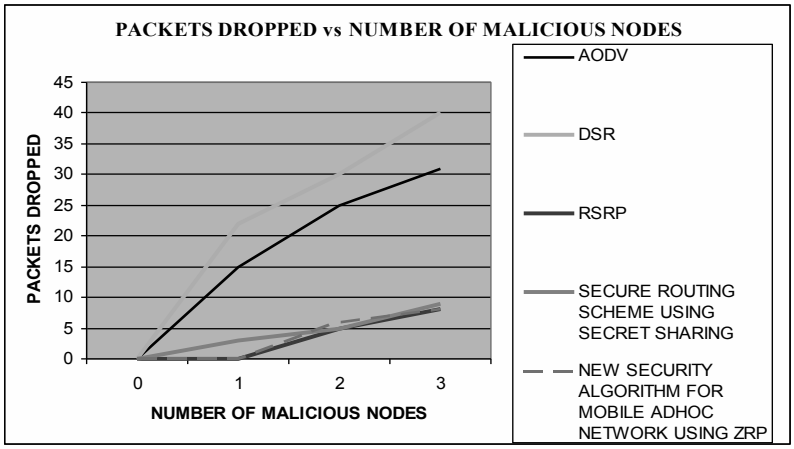

Figure 1. Number of packets dropped vs. number of malicious nodes

B. Computational cost vs. number of nodes

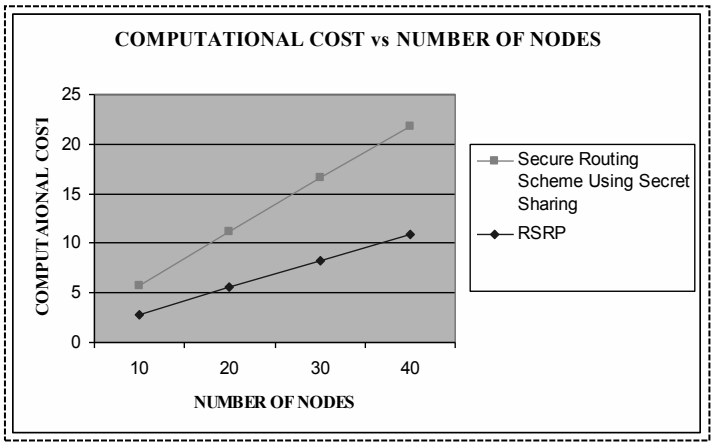

Figure 2. Computational cost vs. number of nodes

In Figure 2 computational cost [1, 3] of proposed protocol *RSRP* (using RSA-CRT for encryption and decryption of messages) is compared only with another ***secure*** *routing protocol using secret sharing* (using RSA for encryption and decryption of messages).

When number of nodes varies from 10 to 40, Computational cost of *Secure Routing Scheme using secret sharing* is always higher than that of *RSRP*, the proposed routing protocol.

C. End to End delay vs. load in MANET

Figure 3 compares end to end delay vs. load amongst *DSR* (a **non-secure** routing protocol), *New Security Routing Protocol Using ZRP* and our proposed protocol *RSRP*. From the figure 3 it has been observed that overall performance of the proposed protocol is far better than *DSR* and *New Security Routing Protocol Using ZRP*. *DSR* being a **non-secure** routing protocol is not able to avoid malicious nodes if present in its path which is responsible for increasing end to end delay in comparison to *RSRP*. Also, performance of *New Security Routing Protocol Using ZRP* is degraded compared to RSRP. This is because of the fact that *Security Routing Protocol Using ZRP* requires extra time delay for creating zone and selecting cluster head which does not happen in case of *RSRP*. This time delay for *Security Routing Protocol Using ZRP* increases as load increases. On the contrary, *RSRP* selects the most secure and stable route depending on some parameters such as trust value, battery power and stability of the nodes present in the route which is not of any concern in case of *Security Routing Protocol Using ZRP*. Performance of the proposed protocol RSRP thus becomes best amongst the three in terms of end to end delay versus load.

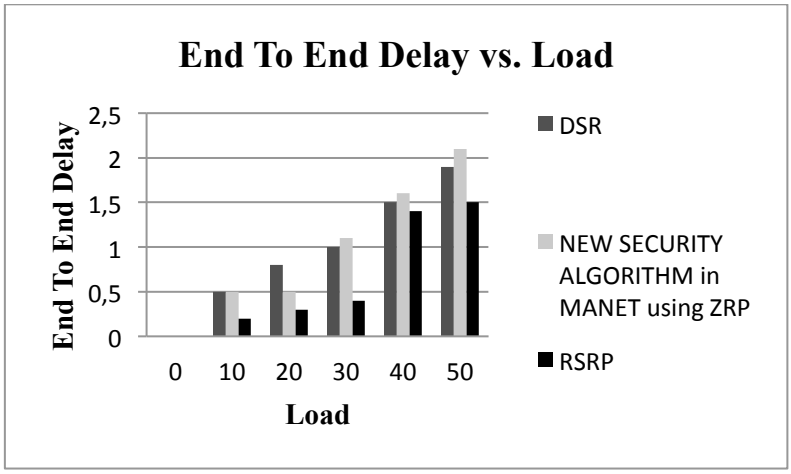

Figure 3. End to End delay vs. load

D. Control packet overheads vs. number of nodes

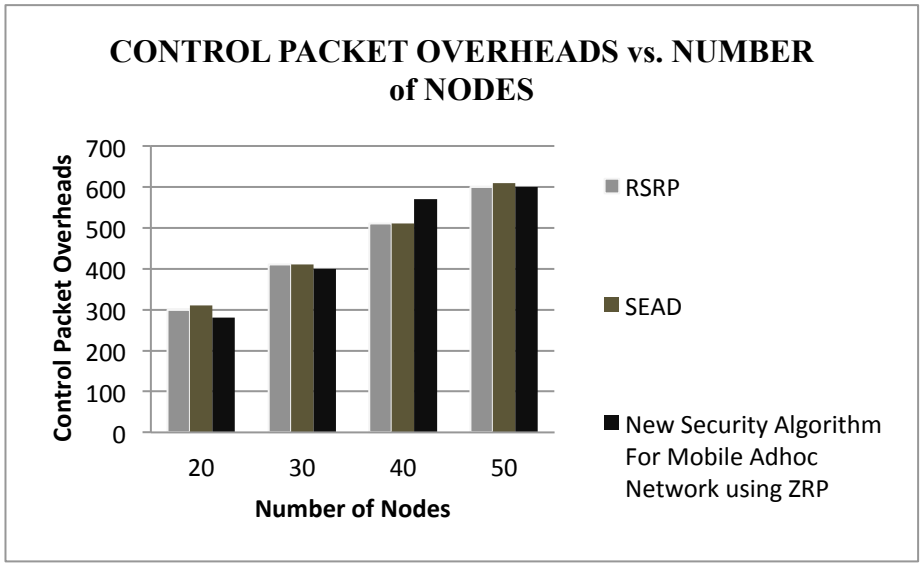

Figure 4. Control packet overheads vs. number of nodes

Figure 4 compares *RSRP* with two **secure** routing protocols *SEAD* and *New security algorithm for MANET using ZRP*. Performance of these three protocols is almost same in terms of control packet overhead vs. number of nodes.

6. Conclusion

Ensuring a secure environment in MANET is a very challenging issue. Securing message transmission normally involves some encryption at source node and decryption at destination node of messages using RSA technique which leads to a large computational overhead. Instead, we use combination of RSA and CRT schemes which reduces the computational overhead to a large extent. Also, the presence of the malicious nodes in the network is the cause of packet loss during transmission of messages through those nodes. Algorithm RSRP tries to identify the set of disjoint routes considered as probable routes between a source-destination pair which are free from those malicious nodes. This action thus reduces the number of packets dropped and in turn improves the performance of the network. Concept underlying Shamir's Secret Sharing scheme is used in RSRP successfully to detect all secure routes from the set of probable routes between a source-destination pair.

Finally, this is to mention that all nodes in a MANET are subject to loss of battery power during message passing/encrypting/decrypting. So, along with stability (inverse of mobility) and trust value, battery power of a node becomes an important issue for selecting a stable and robust route. So, in RSRP we consider weight of a node as the summation of battery power, stability and trust value of that node. Amongst all secure routes detected by Shamir's Secret Sharing principle the route having highest average weighted value has been selected as the final trustworthy and stable route for message transmission.

Performance metrics needed to evaluate our proposed protocol are packet dropped versus number of malicious nodes, computational cost versus number of nodes, end to end delay versus load in terms of number of messages and overhead in terms of number of control packets versus number of nodes. Mobility model is considered here as random waypoint. Performance of the proposed protocol is analyzed using simulation techniques.

This protocol RSRP is compared with two non-secure routing protocols AODV and DSR and also two secure routing protocols i.e.: security algorithm using ZRP [22] and Secure Routing Scheme with Secret Sharing [1]. As expected it shows that packet dropped in case of RSRP is much less compared to AODV and DSR when number of malicious node increases. Comparison with other secure routing protocols shows that RSRP and security algorithm with ZRP shows same and better performance when compared with secure routing scheme with secret sharing.

RSRP is now compared with another secure routing scheme with secret sharing in terms of computational cost as number of nodes increases. It shows performance of RSRP is better than the other one since it uses RSA-CRT scheme for encryption and decryption of messages instead of RSA alone.

Then with increase in load in the network, RSRP shows best performance in terms of end to end delay when compared with DSR (a non-secure routing protocol) and New Security Routing Protocol Using ZRP [22]. In security protocol with ZRP, as load increases number of zones will also increase leading to highest end-to-end delay amongst three.

Comparison in terms of control packet overhead vs. number of nodes shows that difference of performance of three secure routing protocols named as RSRP, New security algorithm for MANET using ZRP and SEAD [7] are negligibly small which implies that number of control packets generated in all the cases are almost equal.

All these comparisons lead us to the conclusion that the overall performance of our proposed protocol RSRP is best from different perspectives, when compared to non-secure routing protocols AODV [13] and DSR [8] as well as three secure routing protocols named as New Security Routing Protocol Using ZRP, SEAD, and Secure Routing Scheme with secret Sharing whereas overhead in terms of number of control packets of RSRP along with three other secure routing protocols remain same.

References

[1] Amuthan, A., & Baradwaj, B. A., Secure Routing Scheme in MANETs using Secret Key Sharing, *International Journal of Computer Applications,* **22**,1, 2011.

[2] Ateniese, G., Santis, A.D., Ferrara, A.L., & Masucci, B., Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, *Proceedings of CCS'06*.Alexandria, Virginia, USA: ACM, 2006.

[3] Broch, J., Maltz, A.D., Johnson, B.D., Hu, C.Y., & Jetcheva, J., A performance comparison of multi-hop wireless ad hoc network routing protocols, *Journal of Mobile Computing and Networking*, 1998, 85–97.

[4] Dang, L., Xu, J., Li, H. & Dang, N., DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks, *Proceedings of 5th IEEE Asia-Pacific Services Computing Conference*,.Hangzhou, China: IEEE Computer Society, 454-461, 2010.

[5] Djenouril, D., Mahmoudil, O., Bouamama, M., Jones, D. L., & Merabti, M., On Securing MANET Routing Protocol Against Control Packet. *Available:www.researchgate.net /.On_Securing_MANET_Routing_Protocol AgainstControlPacket* ,2007.

[6] Grobler, T. L., & Penzhorn, W. T., Fast Decryption Methods for RSA Cryptosystem, *7th AFRICON Conference*.Paris, France: IEEEXPLORE, 2004.

[7] Hu, Y. C., Johnson, D. B., & Perrig, A., SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless AdHoc Networks. *Ad Hoc Networks Journal Elsevier*, **1**, 1, 2003, 175-192.

[8] Johnson, D. B., & Maltz, D. A., Dynamic Source Routing in Ad Hoc Wireless Tomaz Imielinski and Hank Korth (Ed), *Mobile Computing* ,1997, 153-181.

[9] Komninos,N., Dimitrios D., Vergados, Douligeris, C., Authentication in a layered security approach for mobile ad hoc networks , *Journal of Computers & Security,* **26,** 2007, 373-380, *available at www.sciencedirect.com*.

[10] Li, H., Singhal., A Secure Routing Protocol for Wireless Ad Hoc Networks. In *Proceeding of 39th Hawaii International Conference on System Sciences ,* Kauai, Hawaii:IEEE,2006,205a.

[11] Lin, C. H., Lai, W. S., Huang, Y.L., & Chou, M.C., I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks, *Proceedings of International Conference on Multimedia and Ubiquitous Engineering,* Busan, Korea: IEEE, 2008, 102-107.

[12] Lou, W., Liu, W., Zhang, Y., & Fang, Y., SPREAD: Improving network security by multipath routing in mobile ad hoc networks. *Springer Wireless Network,* **15**, 279–294, 2009.

[13] Menaka, A., & Pushpa, M.E., Trust Based Secure Routing in AODV Routing Protocol, *Proceedings of the 3rd IEEE international conference on Internet multimedia services architecture and applications*, Piscataway, NJ, USA: IEEE Xplore, 2009, 268-273.

[14] Perkins, C. E., Belding-Royer, E. M., & Das, S. R., Ad hoc On-Demand Distance Vector (AODV) Routing, *Proceedings of 2nd Workshop on Mobile computing and Applications (WMCSA '99)*, 1999, 90-100.

[15] Perkins.C. E.& Bhagwa P., Highly dynamic destinationsequenced distance-vector routing (DSDV) for mobile computers, *Comp. Commun. Rev*.1994, 234–244.

[16] Rivest, R.L., Shamir, A., &Adleman, L., A method for obtaining digital signatures and public-key cryptosystems., *ACM*, **21**,2, 1978, 120-126.

[17] Sarkar, S., Kisku, B., Misra, S., & Obaidat, M. S., Chinese Remainder Theorem-Based RSA-Threshold Cryptography in MANET using Verifiable Secret Sharing Scheme. *Proceedings of IEEE International Conference On Wireless and Mobile Computing, Networking and Communications,* Marrakech:IEEE, 258-262, 2009.

][18] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., & Belding-Royer., E. M.,A., Secure Routing Protocol for Ad Hoc Networks, *Proceedings of 10th IEEE International Conference on Network Protocols ICNP'02,* Paris, France: IEEE, 78-79, 2002.

[19] Sehgal, P.K., & Nath, R, An Encryption Based Dynamic and Secure Routing Protocol for Mobile Adhoc Network. *International Journal of Computer Science and Security IJCSS,***3**,1, 2009.

[20] Shamir, A.,How to share a secret? *Magazine of Communications of the ACM,* **22,** 11, 1979. doi:10.1145/359168.359176.

[21] Sun, H.M., & Wu, M. E., An Approach Towards Rebalanced RSA-CRT with Short PublicExponent, *Cryptology ePrint Archive: Report 2005/053, Available: http://eprint.iacr.org/2005/053*.

[22] Varaprasad, G., Dhanalakshmi, S., & Rajaram, M., New Security Algorithm for Mobile Adhoc Networks Using Zonal Routing Protocol. *Ubiquitous Computing and Communication Journal (*ubicc.org*), 2008.*

[23] Wang, J. W., Chen, H. C., & Lin, Y. P., A Secure DSDV Routing Protocol for Ad Hoc Mobile Networks**.** In *Proceedings of Fifth International Joint Conference on INC, IMS and IDC*. 2009, 2079-2084.

[24] Wu, C. H., Hong, J.H., & Wu, C. W., RSA Cryptosystem Design Based on the Chinese Remainder Theorem. *Asia and South Pacific Design Automation Conference,* Yokohama, Japan:ACM, 2001, 391-395.

[25] Xia, G., Huang, Z. G., Wang, Z., Cheng, X., Li, W., & Znati, Secure Data Transmission on Multiple Paths in Mobile Ad Hoc Networks, *LNCS Springer-Verlag Berlin Heidelberg .4138,* 2006, 424 – 434 .

[26] Y. Sun, W. Yu, Z. Han, K.J.R. Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, *IEEE Journal on Selected Areas in Communications,* **24**, 2, 305–317, 2006.

Acknowledgement: The authors acknowledge the positive suggestions received from the reviewers of FCDS in improving the quality of the paper.

Received March, 2013